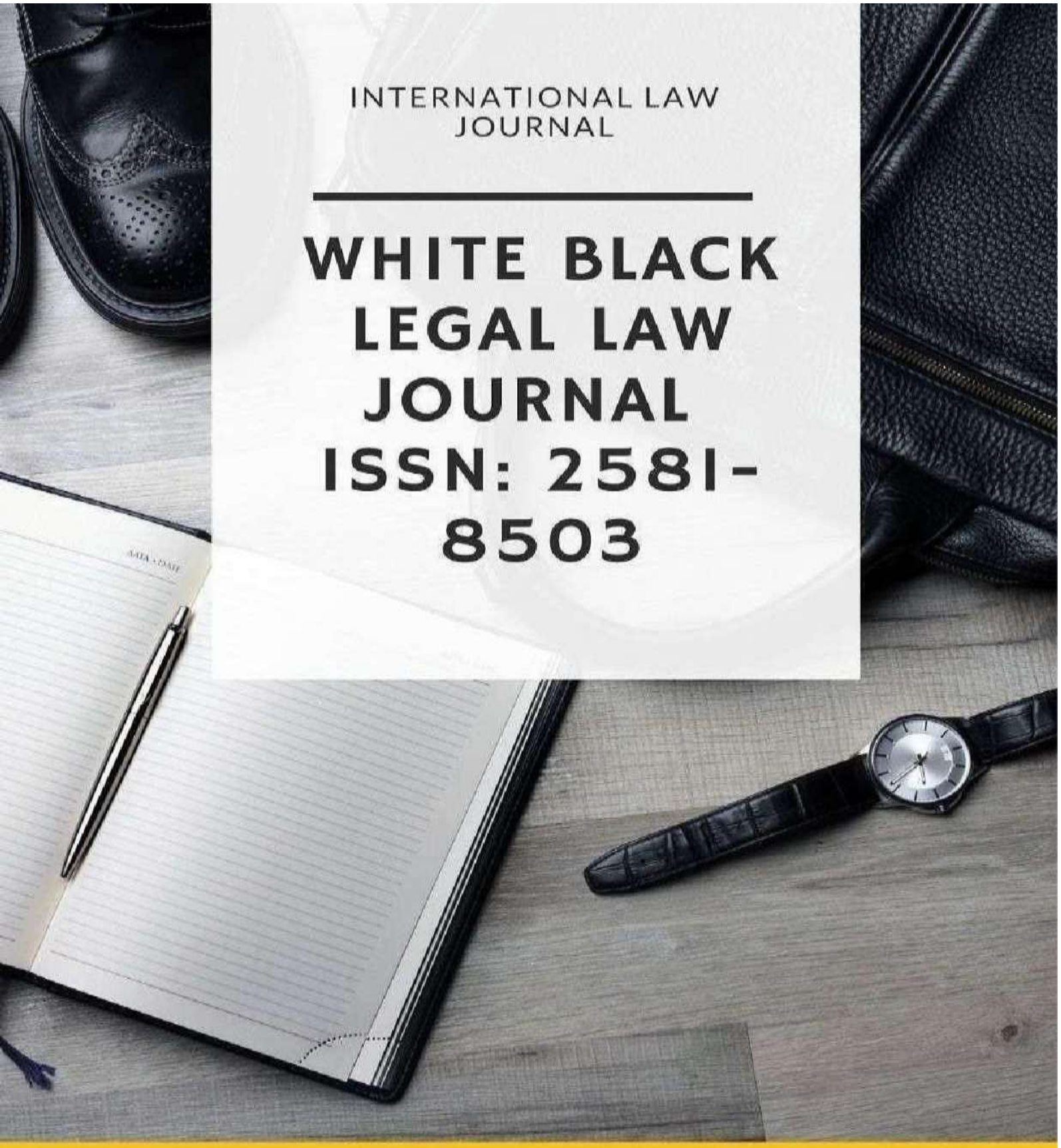

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in ‘Intercountry adoption laws from Uttranchal University, Dehradun’ and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | April 2025 ISSN: 2581-8503

"UN'S APPROACH TO CYBER SECURITY AND AI: CRAFTING INTERNATIONAL LAW FOR EMERGING TECHNOLOGIES"

AUTHORED BY - S.STALIN,
Assistant Professor,
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, School of Law, Avadi, Chennai-600062.

CO-AUTHOR - NOEL LESSLIE THOMAS,
Research Scholar, Crescent School of Law,
B.S Abdur Rahman Institute of Science and Technology, Vandalur, Chennai - 600048.

Abstract:

The rapid proliferation of artificial intelligence (AI) and its integration into cyberspace has introduced unprecedented challenges to global society. As these emerging technologies reshape the cyber security landscape, there is a growing need for robust international legal frameworks to mitigate risks and ensure global peace and stability. The United Nations (UN) has emerged as a key actor in fostering international cooperation and governance in this domain. This paper explores the UN's approach to address cyber security threats posed by AI, with a focus on its efforts to craft a comprehensive international legal order. It examines the UN's role in establishing norms, conventions and resolutions that promote global cyber security and address AI driven threats such as cyber warfare, data breach and the misuse of AI in critical infrastructure. This study critically analyses the challenges the UN faces in regulating AI and cyber security, such as differing national interests, the lack of a universal legal framework, and the rapid evolution of technology. Additionally, it investigates the UN's initiatives in fostering dialogue between member states, private actors and international organizations to develop enforceable and adaptable legal mechanisms. Ultimately, this paper argues that while the UN's approach to crafting an international law in the face of AI related cyber security threat is promising, more cohesive and binding legal instruments are required to effectively govern these technologies in a rapidly changing global environment.

Keywords: Cyber security, Artificial Intelligence, United Nations (UN), International Law, Global governance.

1. Introduction: The Convergence of AI and Cyber security

Artificial Intelligence (AI) has been emerged as a transformative technology across various sectors, significantly impacting the field of cyber security. The integration of AI into cyber defense attack mechanisms has introduced both opportunities and risks[1]. On one hand, AI enhances the ability of organizations and governments to detect, respond to and to prevent cyber attacks more effectively. Machine learning algorithms, predictive analysis and automated threat detection systems allow for quicker identification of vulnerabilities and faster response to attacks.

However, AI has also become a tool for cyber criminals, enabling the development of more sophisticated attacks. AI driven hack, data breach and the creation of malware that can adapt and escalate the complexity of cyber security challenges. The speed at which AI can process vast amounts of data makes it a formidable tool for cyber-attacks, especially in critical sectors like finance, healthcare and national defense.

Figure: 1 Contents covered in this Manuscript

[1]Naeem, AllahRakha. (2024). 2. Cybercrime and the Legal and Ethical Challenges of Emerging Technologies. International journal of law and policy, doi: 10.59022/ijlp.191

Need for International Governance and the Role of the UN:

Given the global nature of cyber security threats, there is a growing recognition that national solutions are insufficient. Cyber-attacks often transcend national boundaries, affecting countries, institutions and individuals across the world. The need for international governance is clear; especially as AI technologies blur the line between state and non-state actors in the cyber warfare.

The United Nations (UN) as the primary global platform for international cooperation has a critical role to play in shaping governance around cyber security and AI[2]. The UN's mandate to promote peace, security and cooperation among nations makes it a natural leader in formulating international norms and governing laws on the use of AI in cyberspace[3]. As AI technologies evolve, so too must the global legal and regulatory frameworks that address their cyber security implications.

2. The United Nations' Role in Global Cyber Security Governance

The United Nations has always focused at the forefront of promoting cyber security at a global level. UN's efforts have been driven by various specialized agencies, including the International Telecommunication Union (ITU), the UN office on Drugs and Crime (UNODC) and the UN Group of Governmental Experts (GGE) on advancing responsible state behavior in cyberspace. These agencies work together to foster dialogue, create standards and promote international cooperation on cyber security[4].

The UN's role has evolved from initial discussions on Internet governance to the broader challenge of cyber security, which now includes addressing the risks posed by AI technologies. The growing interconnectivity of systems, along with the rise of AI in critical infrastructure, makes international cooperation crucial. The UN has sought to bring all member states together along with the other private sector and civil society to build a safer and more secure cyberspace.

[2] M., Kurmangali. (2024). 8. Navigating the Digital Diplomacy Frontier: Multilateral Cooperation in Al Regulation at the UN and EU Levels. doi: 10.26577/irilj.2024.v105.i1.09
[3] UN General Assembly Resolution 70/237 (2015)
[4] UN Group of Governmental Experts (GGE) Reports on Developments in the Field of Information and Telecommunications in the Context of International Security (2010, 2013, 2015)

Key UN Resolutions, Treaties and Initiatives addressing Cyber Security:

Several key initiatives highlight the UN's commitment to global cyber security governance:

UN General Assembly Resolution: The UN General Assembly has adopted numerous resolutions related to cyber security. Notably, the 2015 Resolution on developments in the field of Information and Telecommunications in the context of International security called for the development of voluntary, non-binding norms of responsible state behavior in cyberspace. This resolution laid the groundwork for future discussions on cyber security.

UN GGE on Cyber security: The GGE has been playing a pivotal role in shaping the UN's approach to cyber security. In its 2013 and 2015 reports, the GGE affirmed the International law including the UN Charter applies to cyber space. The group also established a set of norms for responsible state behavior in cyberspace, emphasizing the importance of state sovereignty, non-intervention and the peaceful resolution of disputes.

UN Open-Ended Working Group (OEWG): The OEWG has been established in 2019 as an inclusive platform for all UN member states to discuss cyber security. Its mandate includes advancing international norms, capacity building and exploring how International law applies to state actions in cyberspace.

Global Forum on Cyber Expertise (GFCE): The UN supports global initiatives like the GFCE, which fosters cooperation between governments, international organizations and private entities to build global cyber capacity.

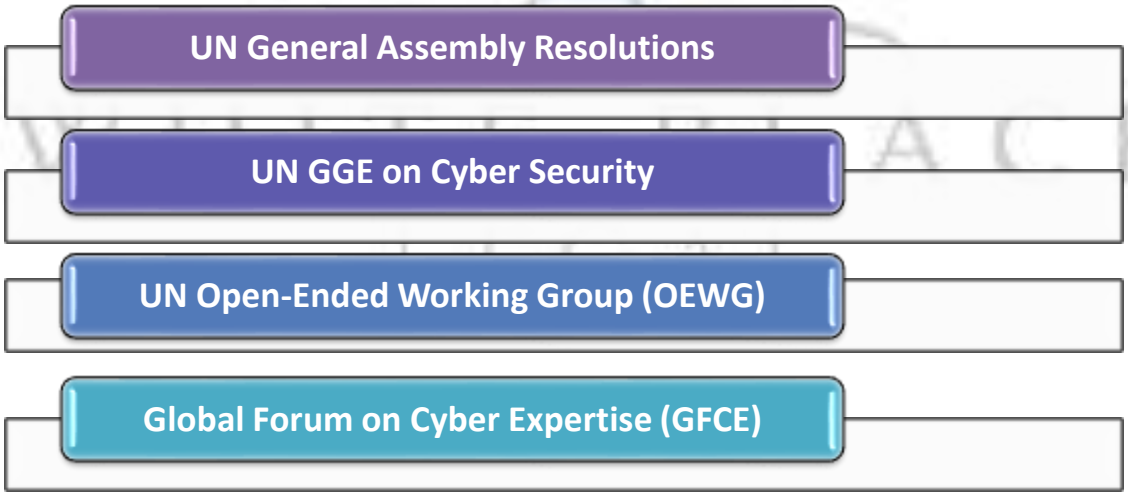

Figure: 2 Key UN Resolutions, Treaties and Initiatives addressing Cyber Security

This initiative highlights the UN's multi-faceted approach to addressing cyber security, with AI posing a new frontier that requires further legal and policy development.

3. Artificial Intelligence in Cyber Space – Opportunities and Threats

AI has a dual role in the realm of cyber security, on the positive side; AI driven tools have revolutionized cyber security defense mechanisms[5]. Predictive algorithms powered by machine learning help to detect anomalies in network behavior, enabling quicker identification of threats. AI driven automation can mitigate the effects of ransom ware attacks, data breach and other cyber crimes by automating responses and enabling real time defense.

However, AI also presents new risks, particularly when it is used as a weapon in cyber attacks. AI powered malware can bypass traditional defense making it harder to detect and neutralize. AI can also be weaponized in espionage operations, allowing for more sophisticated social engineering attacks, phishing campaigns and deep fake technologies that can be used for political or financial gain. The scalability and adaptability of AI make it a powerful tool for state and non-state actors in conducting cyber warfare.

Case Studies of AI driven Cyber attacks or Defense Systems:

AI in Phishing: AI has been used to improve phishing attacks, making them more personalized and difficult to detect by analyzing social media and communication patterns. AI can craft highly convincing phishing emails that are tailored to individual target increasing the chances of successful breach.

AI Powered Malware: In 2017, AI powered malware was demonstrated at a cyber security conference showing how malware could evolve and adapt to defense autonomously. The malware learned from its environment adjusting its strategies to evade detection.

AI in Cyber defense: Large Organizations and governments have increasingly adopted AI driven defence systems. For example, the US department of defence has implemented AI based cyber security solutions to protect critical infrastructure, using algorithms to predict attack and autonomously respond to threats in real time.

[5] Jialing, Liu. (2024). 1. Artificial Intelligence and International Law: The Impact of Emerging Technologies on the Global Legal System. Economics, law and policy, doi: 10.22158/elp.v7n2p73

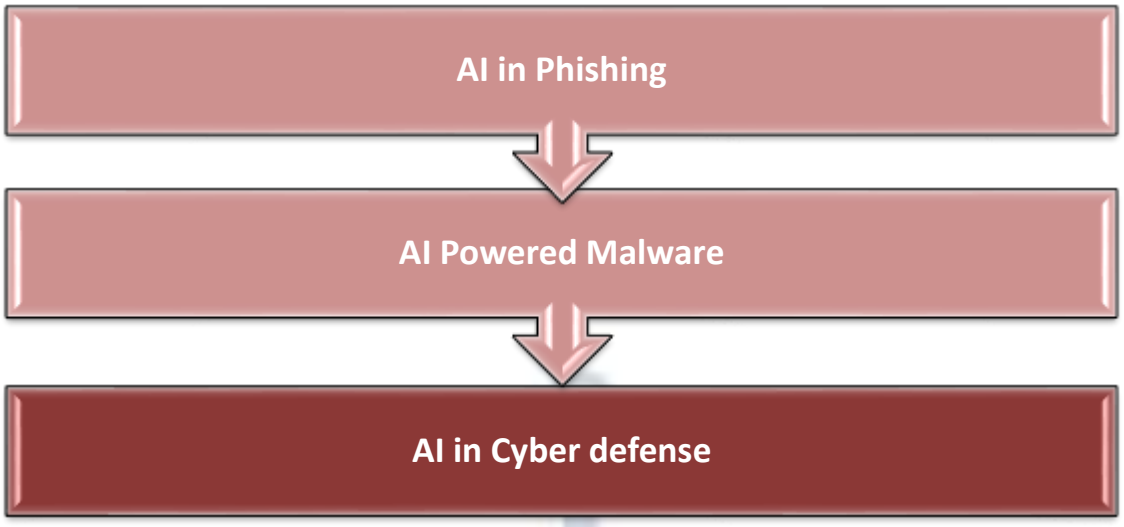

***Figure: 3 Case* studies of AI driven Cyber-attacks or Defense Systems**

These examples demonstrate both the positive and negative potentials of AI in cyber security, highlighting the need for international governance[6].

4. Existing International Legal Frameworks for Cyber Security

The existing International legal framework for cyber security is fragmented, with no single, binding international treaties specifically addressing the governance of AI driven cyber security threats. Several international instruments and frameworks address cyber security more broadly, but they fall short of providing comprehensive regulations of AI related cyber threats.

The Budapest Convention on Cyber Crime (2001): This convention from the Council of Europe is the only binding international treaty on cybercrime. While it focuses primarily on cyber crime rather than cyber security, it has provided a framework for international cooperation on cyber investigations, evidence collection and law enforcement coordination.

The Tallinn Manual on the International Law applicable to Cyber Warfare (2013): Although not a binding document, the Tallinn Manual provides an authoritative interpretation of how the international law, particularly the laws of armed conflict applies to cyber space. It discusses cyber attacks, including those powered by AI, and their potential to trigger international legal consequences under the laws of war.

The Paris Call for Trust and Security in Cyber space (2018): Launched by France, this non-binding declaration has garnered support from over 70 countries and private sector actors. It

[6] Clara, Pettoello-Mantovani. (2024). 3. Cybercrimes: An Emerging Category of Offenses within the Frame of the International Criminal Court Jurisdiction. International journal of law and politics studies, doi: 10.32996/ijlps.2024.6.2.2

calls for the development of norms to protect critical infrastructure, prevent cyber attacks on the electoral process and strengthen international cooperation on cyber security.

Gaps and limitations in current legal mechanisms for addressing AI-Related Cyber threats:

While the aforementioned frameworks have made strides in fostering international cooperation on cyber security, they fall short in addressing the specific challenges posed by AI-driven cyber threats. Some of the key limitations include:

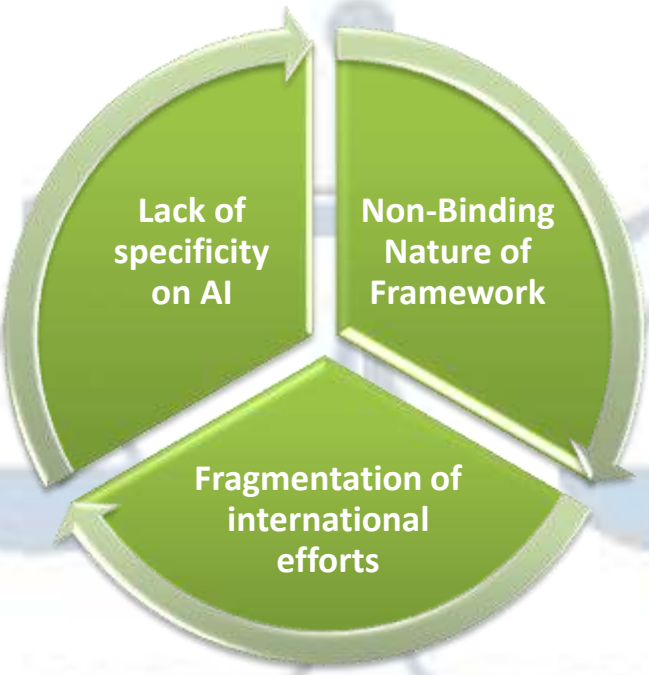

Figure: 4 **.Gaps and limitations in current legal mechanisms for addressing AI-related Cyber threats.**

Lack of Specificity on AI: Existing treaties and conventions do not address the unique challenges of AI, such as the autonomous decision making in cyber attacks or the use machine learning to bypass cyber defence. This creates a legal vacuum for emerging AI technologies[7].

Non-Binding Nature of Framework: Many international cyber security frameworks, including the UN's norms of state behavior in cyberspace, are voluntary and non-binding. This limits their enforcement and accountability, especially in the context of AI-driven cyber attacks that may not be covered by existing laws.

[7] Naek, Siregar. Desy, Churul, Aini., Rehulina, Rehulina., Agit, Yogi, Subandi., Isroni, Muhammad, Miraj, Mirza. (2024). 4. The Use of Artificial Intelligence in Armed Conflict under International Law. Hasanuddin Law Review, doi: 10.20956/halrev.v10i2.5267

Fragmentation of international efforts: Different regions have adopted varying approaches to cyber security resulting in lack of cohesive international governance. For example, the European union's General Data Protection Regulation (GDPR) emphasizes data protection, while other regions may prioritize different arena of cyber security.

This rapid development of AI technologies, coupled with growing sophistication of cyber-attacks, highlights the need for more comprehensive, binding, and AI specific international legal frameworks. The UN's role in leading this effort will be critical in ensuring global cyber security in an increasingly AI driven world[8].

5. Challenges in crafting AI-Specific Cyber security laws

Artificial intelligence (AI) is advancing at an unprecedented rate, making the regulation of AI-Specific cyber security laws a complex challenge. AI Systems Continually learn, adapt and evolve, which means any regulatory framework must be flexible enough to accommodate technological innovations without stifling progress. This rapid pace of development complicates the ability to forecast potential risk and vulnerabilities associated with AI, particularly in cyber security. Regulatory body must strike a balance between fostering innovation and ensuring robust security measures. The unpredictability of AI evolution also presents difficulties in defining clear legal responsibilities for developers and regulators[9].

Diverging National interests and legal standards

A significant challenge in crafting international laws and AI and cyber security is the divergence of national interests and legal standards. Different countries have varying priorities and capacities for regulating AI, depending on their technological capabilities and political agendas. For instance, while some nations emphasize data protection and privacy, others may focus on the economic potential of AI, leading to differing regulatory approaches. This lack of uniformity created hurdles for international cooperation, as countries, as countries may resist adopting laws that conflict with their domestic policies. The disparity between advanced and developing countries in terms of technological infrastructure and cyber security readiness further complicates efforts to craft globally applicable laws[10].

[8] Ashutosh, Singh. (2024). 13. The Role of International Law in Addressing Transnational Cybersecurity Threats: Challenges and Opportunities. doi: 10.36676/ijl.v2.i2.07
[9] Cemal, Tosun. (2023). 5. AI and international law. doi: 10.4337/9781800379220.00013
[10] Kinfe, Micheal, Yilma. (2023). 9. Emerging Technologies and Human Rights at the United Nations. IEEE Technology and Society Magazine, doi: 10.1109/mts.2023.3241297

The Challenge of creating binding enforceable International Laws

One of the most pressing issues in cyber security governance is the lack of binding and enforceable international laws, particularly in the context of AI. Current international agreements and norms are largely non-binding, which limits their effectiveness in holding states and non-state actors accountable for AI-driven cyber attacks. The challenge lies in persuading states to agree in a binding framework that addresses the complex nature of AI in cyber security while respecting national sovereignty. Moreover, enforcement and mechanisms for such laws remain a critical challenge, as the global nature of cyberspace makes it difficult to impose legal consequences to an actors operating across different jurisdictions.

6. The UN's Collaborative efforts: Engaging member States and Private actors

The United Nations (UN) has recognized that addressing the challenge posed by AI and cyber security requires a collaborative approach involving multiple stakeholders. To this end, the UN has actively engaged member states, international organizations and the private sector in its efforts to develop a cohesive global strategy. Through forums such as the Open Ended Working Group (OEWG) on cyber security and the Group of Government Experts (GGE), the UN has facilitated discussions among states to promote responsible behavior in cyberspace.

Additionally, the UN has worked with private sector actors, including tech companies, to ensure that industry expertise is leveraged onto the development of cyber security standards. Initiatives like the Global Forum on Cyber Expertise (GFCE) have helped to build bridges between governments, industry leaders and civil society, fostering a collaborative environment for addressing AI-related cyber threats.

Multi-Stakeholder Collaboration in Cyber Security Governance

The growing complexity of AI technologies and the increase in global nature of cyber threats necessitates a multi-stakeholder approach to cyber security governance. Engaging a wide range of actors, governments, private companies, international organizations and civil society ensures that diverse perspectives are considered in the development of the policy standards. The private sector in particular plays a critical role in AI and cyber security, as many of the technologies used for cyber defence and attack originate from private companies[11].

[11] Sorin, Topor. (2023). 11. The interaction of emerging technologies with the legal field. International Journal of

Multi-stakeholder collaboration also promotes greater transparency and accountability, as it encourages the sharing of information, best practices and resources among different actors. This collaborative approach is essential for addressing the cross-border nature of cyber security threats, ensuring that no single country or organization is solely responsible for safeguarding global cyberspace.

7. Role of the UN in Setting Global norms for AI

The United Nations has been playing a pivotal role in establishing global norms and its ethical standards for the use of AI in cyber security[12]. The UN has consistently emphasized the need for responsible behavior in cyber space and this extends to the use of AI technologies. Through initiatives such as the GGE and the OEWG, the UN has sought to create norms that guide the development and deployment of AI technologies in a way that promotes peace and security.

The UN's normative efforts focus on ensuring AI is used in a manner that respects human rights, avoids exacerbating conflicts and safeguards critical infrastructure. These norms also encourage transparency in AI development, requiring states and private actors to open about how AI systems are used in cyber security operations. The UN's emphasis on ethical AI use is designated to prevent the misuse of AI for malicious purposes such as launching AI- driven cyber attacks or employing AI in cyber espionage.

UN Recommendations and Guidelines for responsible AI use

In its pursuit of global cyber security, the UN has issued several recommendations and guidelines for the responsible use of AI. These include calls for transparency in AI algorithm design in aligning the ethical use of AI in Cyber defence and the importance of accountability in the deployment of AI systems. The UN also encourages states to adopt measures that promote the peaceful use of AI in cyber space and avoid its weaponization.

The UN's guidelines stress out the importance of adhering to the International law in the use of AI for cyber security purposes, particularly in the principles of state sovereignty, non-intervention and the peaceful settlement of disputes among member states. These

Legal and Social Order, doi: 10.55516/ijlso.v3i1.157

[12] Ashutosh, Singh. (2024). 13. The Role of International Law in Addressing Transnational Cybersecurity Threats: Challenges and Opportunities. doi: 10.36676/ijl.v2.i2.07

recommendations aim to create a framework where AI technologies have been developed and used in a manner that contributes to global stability and security[13].

8. UN Initiatives on Capacity Building and International Cooperation

The UN has launched several initiatives aimed at capacity building in cyber security. One of the key programs is the Global Cyber security Agenda (GCA), which is focused on enhancing cyber security capabilities across the globe. The GCA promotes international cooperation, technical assistance, and sharing the best practices, particularly to support countries with limited cyber security infrastructure.

The UN also supports capacity building efforts through Cybercrime Capacity Building Programme, which provides training and resources to help developing countries improve their cyber defence systems. This program aims to empower nations to protect their critical infrastructure from AI driven cyber attacks and ensure to have the tools necessary to participate in global cyber security efforts.

Promoting International Cooperation and Information –Sharing Mechanisms

International cooperation is central to the UN's approach to cyber security governance. The UN has promoted several initiatives aimed at fostering cross-border collaboration, such as the establishment of Computer Emergency Response Team (CERTs) and creation of platforms for information sharing among states. These mechanisms allow countries to share threat intelligence, coordinate responses to cyber incidents and collectively address AI driven cyber threats.

By facilitating cooperation among member states, the UN seeks to build a global community that is better equipped to handle the challenges posed by AI in cyber security. Information sharing initiatives are particularly important in mitigating the risks associated with AI, as they enable countries to stay informed about emerging threats and develop coordinated responses.

[13] Dmitry, P., Vasilyev. (2023). 17. Formation of International Artificial Intelligence Governance Regimes: Key Trends and Main Actors. Obŝestvo: politika, èkonomika, pravo, doi: 10.24158/pep.2023.8.9

9. Future Prospects: Developing a Comprehensive's International Legal Order

As AI continues to reshape the cyber security landscape, there is a growing need for a comprehensive international legal framework that addresses the unique challenges positioned by AI driven cyber threats. The UN is well positioned to lead the development of such a framework, given its experience in fostering international cooperation and its role in promoting peace and security[14].

A cohesive legal order would need to address several key areas, including the regulation of AI in cyber warfare, the protection of critical infrastructure from AI driven attacks and the establishment of norms in cyber security. This framework would also need to be binding and enforceable ensuring that states and non-state actors are held accountable for their actions in cyber space[15].

Figure 5: Future Prospects: Developing a Comprehensive's International Legal Order

Recommendations for strengthening International Laws and ensuring Global Security

To strengthen international laws governing AI and cyber security, several steps must be taken:

Develop Binding Norms: The UN should work with member states to develop binding norms

[14] Cemal, Tosun. (2023). 20. International human rights as 'ideal' AI governance. doi: 10.4337/9781800379220.0001

[15] Huaiyuan, Xu. (2023). 22. Legal Exploration of AI Face-Changing Technology. doi: 10.54097/ajmss.v2i3.8939

for AI use in cyber security, ensuring that these norms are enforceable and backed by clear accountability mechanisms.

Enhance Multilateral Cooperation: The UN should continue to promote multilateral cooperation, encouraging countries to work together on developing legal frameworks that address the global nature of AI-driven cyber threats.

Promotion of Ethical AI use: The UN should establish clear ethical guidelines for AI use in cyber security, focusing on transparency, accountability and the protection of human rights.

Build Capacity: Developing nations should be supported through capacity building programs to ensure they can effectively participate in global cyber security governance.

10. Conclusion

The UN's efforts in addressing the challenges constituted by AI and cyber security have made significant strides in fostering international cooperation and developing global norms. However, as AI technologies continue to evolve, there is an urgent need for a binding and comprehensive international legal framework that addresses the unique threats posed by AI in cyber space. The UN's role in this process will be crucial, as it works to promote peace, security, and ethical AI use through its collaborative efforts along with member nations; the private sector and the international organizations.

In Conclusion, future of cyber security governance in AI era depends on the continued engagement of all stakeholders in the development of international laws that are both flexible and enforceable. The UN must remain at the forefront of these efforts, ensuring that cyber space remains a secure environment for all nations in the face of AI-driven threats.

References:

1. Naeem, AllahRakha. (2024). 2. Cybercrime and the Legal and Ethical Challenges of Emerging Technologies. International journal of law and policy, doi: 10.59022/ijlp.191[16]
2. Jialing, Liu. (2024). 1. Artificial Intelligence and International Law: The Impact of Emerging Technologies on the Global Legal System. Economics, law and policy, doi: 10.22158/elp.v7n2p73

3. Clara, Pettoello-Mantovani. (2024). 3. Cybercrimes: An Emerging Category of Offenses within the Frame of the International Criminal Court Jurisdiction. International journal of law and politics studies, doi: 10.32996/ijlps.2024.6.2.2
4. Naek, Siregar. Desy, Churul, Aini., Rehulina, Rehulina., Agit, Yogi, Subandi., Isroni, Muhammad, Miraj, Mirza. (2024). 4. The Use of Artificial Intelligence in Armed Conflict under International Law. Hasanuddin Law Review, doi: 10.20956/halrev.v10i2.5267
5. Cemal, Tosun. (2023). 5. AI and international law. doi: 10.4337/9781800379220.00013
6. Kinfe, Micheal, Yilma. (2023). 6. Emerging Technologies and Human Rights at the United Nations. IEEE Technology and Society Magazine, doi: 10.1109/MTS.2023.3241297
7. M., Kurmangali. (2024). 8. Navigating the Digital Diplomacy Frontier: Multilateral Cooperation in Al Regulation at the UN and EU Levels. doi: 10.26577/irilj.2024.v105.i1.09
8. Kinfe, Micheal, Yilma. (2023). 9. Emerging Technologies and Human Rights at the United Nations. IEEE Technology and Society Magazine, doi: 10.1109/mts.2023.3241297
9. Sorin, Topor. (2023). 11. The interaction of emerging technologies with the legal field. International Journal of Legal and Social Order, doi: 10.55516/ijlso.v3i1.157
10. Ashutosh, Singh. (2024). 13. The Role of International Law in Addressing Transnational Cybersecurity Threats: Challenges and Opportunities. doi: 10.36676/ijl.v2.i2.07
11. Cristos, Velasco. (2022). 14. Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. ERA Forum, doi: 10.1007/s12027-022-00702-z
12. Dmitry, P., Vasilyev. (2023). 17. Formation of International Artificial Intelligence Governance Regimes: Key Trends and Main Actors. Obŝestvo: politika, èkonomika, pravo, doi: 10.24158/pep.2023.8.9
13. (2022). 18. Cybersecurity Vis-A-Vis Artificial Intelligence: An Analysis of the International Conventions. doi: 10.1007/978-981-19-4052-1_36
14. Alexandru, Georgescu. (2022). 19. Cyber Diplomacy in the Governance of Emerging AI Technologies - A Transatlantic Example. International Journal of Cyber Diplomacy, doi: 10.54852/ijcd.v3y202202

15. Cemal, Tosun. (2023). 20. International human rights as 'ideal' AI governance. doi: 10.4337/9781800379220.00018
16. Huaiyuan, Xu. (2023). 22. Legal Exploration of AI Face-Changing Technology. Doi: 10.54097/ajmss.v2i3.8939

Legislations and Covenants:

1. United Nations Charter (1945)
2. International Covenant on Civil and Political Rights (ICCPR, 1966)
3. International Covenant on Economic, Social and Cultural Rights (ICESCR, 1966)
4. Budapest Convention on Cybercrime (2001)
5. Tallinn Manual on the International Law Applicable to Cyber Warfare (2013)
6. UN General Assembly Resolution 70/237 (2015)
7. UN Group of Governmental Experts (GGE) Reports on Developments in the Field of Information and Telecommunications in the Context of International Security (2010, 2013, 2015)
8. Convention on Certain Conventional Weapons (CCW, 1980)
9. Shanghai Cooperation Organization (SCO) Agreement on Cyber security (2017)
10. European Union’s General Data Protection Regulation (GDPR, 2018)
11. UN Sustainable Development Goals (SDGs, 2015)