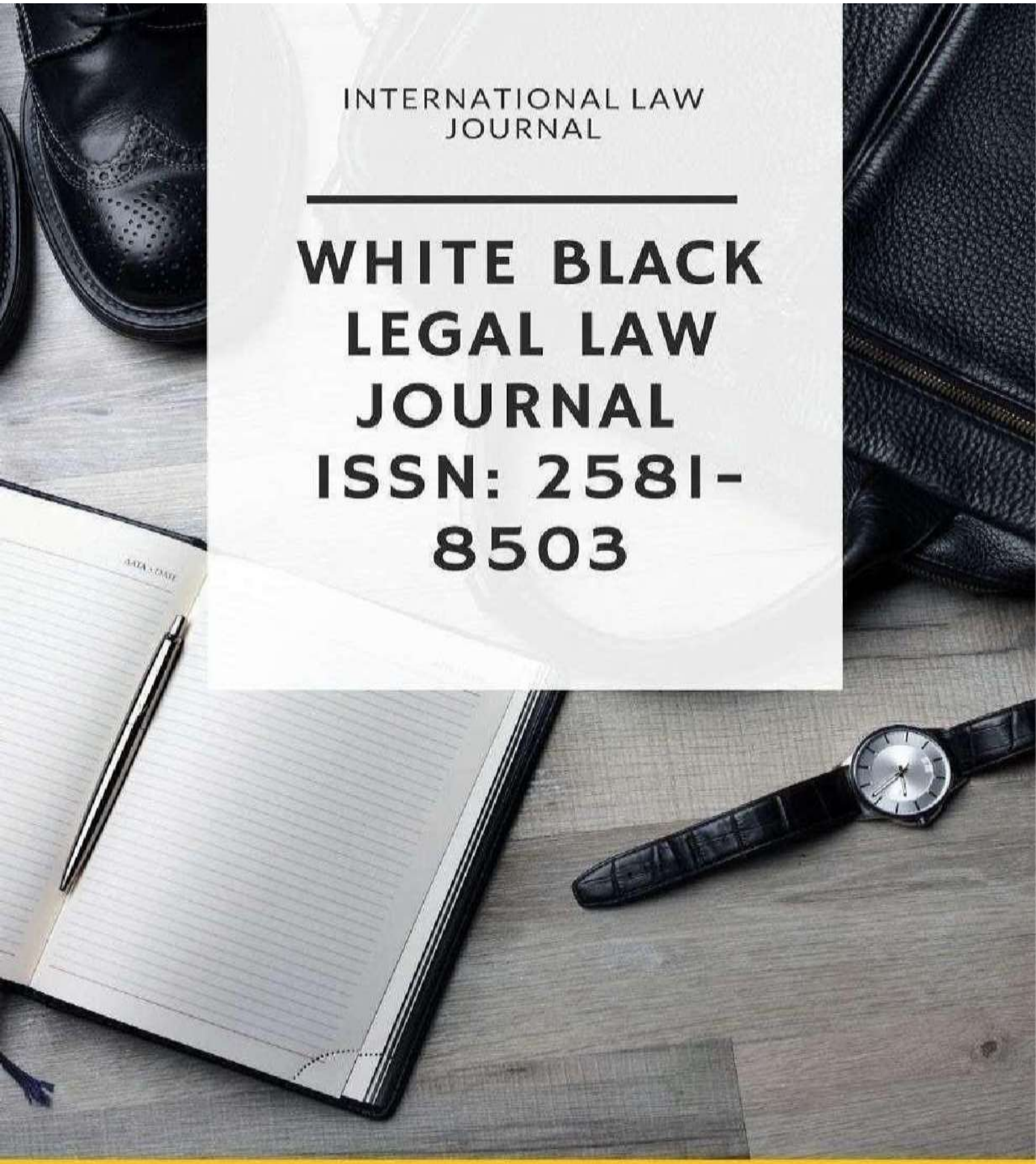

INTERNATIONAL LAW JOURNAL

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.

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

CYBER SECURITY AND AI UNDER INTERNATIONAL LAW

AUTHORED BY - ARUNDHATI SINGH

As digital technologies proliferate and more facets of our lives migrate to cyber-connected systems, robust statutes safeguarding computer networks and data repositories against unauthorized ingress and cyberattacks have become imperative. Myriad cybersecurity regulations strive to shield critical infrastructure, intellectual property, and sensitive personal information from compromised security, data breaches, and exploitation by illicit actors. However, the rapid evolution of hacking techniques, decentralized architectures, and sophisticated malware payloads have rendered some existing legal frameworks insufficient and antiquated. While foundational laws criminalizing unauthorized access, data theft, and system disruption provide an elementary layer of defence, keeping pace with the advanced persistence threats of motivated cybercriminals and state-sponsored offensive operations necessitates legislative agility and technologically informed precautions. By implementing nuanced, proactive laws that deter would-be threat actors while empowering companies to share actionable threat intelligence with appropriate governmental entities, lawmakers can bolster cyber defences across private and public sectors. Nevertheless, privacy advocates caution against the overreach of government surveillance and monitoring capacities even in pursuit of enhanced security. Therefore, updating cybersecurity statutes requires a delicate balance, one that protects digital assets and infrastructure without compromising civil liberties.

The emergent capabilities of artificial intelligence portend formidable perils for cybersecurity as sophisticated algorithms can potentiate unparalleled attacks that thwart conventional defences. AI-enabled adversaries can clandestinely case digital infrastructure, probe for zero-day vulnerabilities, and unleash polymorphic malwares – machine learning suites that continuously morph evasion techniques. Swarms of Bots endowed with natural language processing can convincingly impersonate humans, socially engineering access through spear-phishing emails or duping gatekeepers. Deepfakes fabricated through generative adversarial networks allow assumption of trusted identities via falsified biometrics, while quantum-accelerated decryption shatters encryption shields. To counter such shape-

shifting threats, cyber protectors must pioneer robust solutions: defensive AI that sniffs out subtle indicators of compromise; explainable AI that elucidates the opaque workings of learning systems; blockchain-enabled verification of identities and assets; and resilient engineering of complex networks. As machine learning expands the attack surface, international concord on AI safety standards, cyber ethics, and rapid-response information sharing will prove critical. By imbuing machines with human-aligned values, farsighted governance can harness AI's power for civic progress, not peril. With technological innovation come profound responsibilities – if nations and citizens jointly cultivate a culture of digital conscience, artificial intelligence may uplift humanity.

Though an omnibus global accord on cybersecurity remains elusive, nations have endeavoured to foster robust networks of bilateral and multilateral pacts tethered to prevailing frameworks of international law. Operating under the aegis of the United Nations, member states espouse an array of voluntary norms that champion terrestrial stability in the cyber domain - dutifully marshalling resources to combat threats, hardening critical infrastructure against attack, and mutualizing essential insights into the tradecraft of malign actors. While lacking coercive authority, these prescriptions aim to cultivate a culture of cooperation and continuity across transnational informational ecosystems. Regional alliances like the Association of Southeast Asian Nations have amplified the UN standards through binding Cybersecurity Resolutions. Beyond prescriptive norms, settled tenets of humanitarian and warfare law apply - holding state forces accountable for violations of digital sovereignty or collateral damage against civilians. As the permeability of borders steadily evaporates in the interconnected Internet, cyber stability relies on supra-national pacts and shared doctrine to steer state conduct away from dangerous disruption. A globe-spanning digital concord - one that reconciles security with liberty - may remain distant, but patient diplomacy can bring it incrementally nearer.

Moreover, domestic cybersecurity statutes must accord with international human rights law, upholding civil liberties like privacy, expression, and access to information that traverse borders along fibre optic currents. The reterritorialized architecture of the internet necessitates multilateralism to balance security with liberty across the global village. Numerous technologists have championed a "Digital Geneva Convention" that would extend humanitarian protections to cyberspace, safeguarding civilians from indiscriminate hacking, digital weapons proliferation, and infrastructure

attacks that imperil the innocent. While consensus on such instruments remains nascent, extant frameworks, like the Budapest Convention on cybercrime cooperation, evince the possibility of pluralistic global governance. Scholars argue that the communal ethos and decentralization innate to the internet could model an organically evolving legal order, shaped by collaborative design and grounded in mutual restraint. Though yawning lacunae persist, the foundations have been laid through international law and cooperative forums for jointly confronting emerging threats while securing universal rights on the digital frontier. With patient faith in multi-stakeholder dialogue, mutual security and liberty need not be zero-sum outcomes.

The purported intent of international law is to impose standards of conduct on sovereign nation-states and mitigate overt martial clashes. However, learned scholars debate the actual potency of international legal frameworks in circumscribing organized state-sanctioned violence.

The advent of sophisticated artificial intelligence technologies is poised to substantially influence the evolution and practical implementation of international law frameworks. Both the interpretative lens through which existing statutes and conventions are applied, as well as the very process of enforcing compliance and accountability for violations may be impacted by incorporation of algorithmic systems and predictive analytics. In addition, the emergence of AI-enabled capabilities raises novel and complex regulatory challenges for the international community related to constraining potentially dangerous uses and applications, including autonomous weapons platforms and intrusive surveillance algorithms. There is a risk that unchecked AI development by a handful of technology leaders could destabilize regional dynamics and undermine human rights in absence of governance guardrails. The proliferation of AI globally, if mishandled, contains seeds of greater interstate mistrust, escalatory arms races in new domains, and opportunities for unlawful covert operations difficult to attribute. Getting ahead of these risks proactively through evolving international law will prove critical. For laws to be effective, they must dynamically reflect new realities introduced by technologies like AI. Promoting beneficial uses while prohibiting malicious ones will require nuanced governance combining ethical norms, codes of conduct, and adaptively designed prohibitions.

The advent of sophisticated artificial intelligence technologies is poised to substantially influence the evolution and practical implementation of international law frameworks. Both the interpretative lens

through which existing statutes and conventions are applied, as well as the very process of enforcing compliance and accountability for violations may be impacted by incorporation of algorithmic systems and predictive analytics. In addition, the emergence of AI-enabled capabilities raises novel and complex regulatory challenges for the international community related to constraining potentially dangerous uses and applications, including autonomous weapons platforms and intrusive surveillance algorithms. There is a risk that unchecked AI development by a handful of technology leaders could destabilize regional dynamics and undermine human rights in absence of governance guardrails. The proliferation of AI globally, if mishandled, contains seeds of greater interstate mistrust, escalatory arms races in new domains, and opportunities for unlawful covert operations difficult to attribute. Getting ahead of these risks proactively through evolving international law will prove critical. For laws to be effective, they must dynamically reflect new realities introduced by technologies like AI. Promoting beneficial uses while prohibiting malicious ones will require nuanced governance combining ethical norms, codes of conduct, and adaptively designed prohibitions.

The emergence of sophisticated cyber and artificial intelligence technologies has generated unprecedented dilemmas for the international legal order. As techniques become more refined, so too do the menaces posed by illicit state-supported hacking, cyberwarfare, and potential misuses of AI. However, the existing corpus of international law has been sluggish to evolve and expand to effectively govern these complex and multidimensional issues. The rapid pace of technological advancement in these areas seems to have outpaced the relatively slower development of binding legal conventions and norms. This lag poses risks of unregulated "gray areas" arising quicker than the international community can build consensus on their governance.

International humanitarian law provides established regulations regarding permissible and prohibited actions in the context of armed conflicts. However, the applicability of these statutes to offensive cyber operations remains legally ambiguous and open to dispute among experts. For example, legal specialists involved in the Tallinn Manual[1] negotiations disagreed on whether a cyber operation that directly induces physical harm could constitute a prohibited attack on civilian infrastructure. Some argue if cyber activities are not explicitly defined as "attacks", they may reside in a grey area not clearly covered under existing humanitarian law precepts. This illustrates the difficulties of directly translating the established laws of conventional warfare to the relatively novel domain of

cyberwarfare.

The United Nations and affiliated regional alliances have drafted and promoted voluntary guidelines encouraging accountable conduct by sovereign states within the cyber arena. However, the inherently political nature of these multilateral forums implies that coercive enforcement mechanisms are feeble at best, and narrow national interests of influent countries take precedence. For instance, negotiations within the UN Group of Governmental Experts faltered due to unreconciled positions between the United States and Russia concerning state prerogatives over domestic information ecosystems and cyber systems deemed critical infrastructure[2]. The nonbinding status of these normative principles seemingly does little to deter intensifying cyber intrusions attributed to state-sponsored entities. Absent binding prohibitive deterrents, attempts to foster transparency, confidence-building measures, and global consensus around responsible state behaviour in cyberspace remain largely hortatory gestures. The ambitious aim of formulating a mutually acceptable "rules of the road" to regulate cyberspace remains elusive, complicated by national security interests and the domain's unique attributes.

AI tech with military applications, like autonomous weapons, also lack comprehensive governance. While 26 countries[3] have called for a ban on lethal autonomous weapons, progress on formal regulations is slow. The opacity around development of military AI breeds mistrust and uncertainty. Ambiguity persists on legal liability frameworks for autonomous systems' actions.

It is unlikely that strict international legal frameworks will be established to regulate the dynamics of growing cyber and AI armaments given the ongoing hostility between the world's leading geopolitical countries. Using voluntary codes of ethics, interstate transparency initiatives, and informal non-proliferation agreements as leverage for soft law paths would be more practical first steps. Global cooperation will be essential if international laws are to keep up with the extraordinary systemic risks brought about by these increasingly advanced technologies. Collectively binding action, however, is likely to face ongoing challenges due to competing national security objectives and rivalries between powerful nations. Even first attempts at taking actions to boost confidence encounter significant obstacles in the absence of a common urgency. Instead of fostering unity, major powers' posturing for advantage in the AI and cyber domains deepens divisions. It will take astute diplomacy and

strategic patience to find technical parameters that are acceptable to all parties, highlight shared dangers, and create adaptable norms that have enough support to eventually become self-enforcing. However, in the absence of a crisis that highlights the pressing need for cooperation, competing interests may prevent solutions. The fragmentation of international law across areas such as cyberspace, air, sea, and space is a challenge. It is necessary to update laws, standards, and confidence-boosting measures in order to incorporate AI and cyber security into cogent legal frameworks. In order to provide strategic stability, this calls for linking technical innovation with its governance.

Impact of AI in International law is vast. Laws established for humans might need to be emphasised when they apply to algorithms that are intelligent and autonomous systems. Who is legally liable, for instance, if an AI weapon system violates the law governing armed conflict? Is human rights law applicable to algorithms? Responsibility concerns grow hazier with new technologies. AI could assist with the previously unattainable magnitude of legal corpus analysis, including case histories, arbitration records, and treaties. This can facilitate uniform application of the legislation. If the AI takes inferences from faulty datasets, it also poses the risk of sustaining ingrained prejudices. It is essential to mitigate bias when training legal AI.

The use of AI by authorities for profiling, surveillance, and predictive policing may jeopardise citizens' right to privacy. The topic of regulating government use of AI technology to prevent abuse is now being discussed in international policy debates. export limitations are being considered on AI surveillance techniques that are obtrusive. Concerns about accountability, stability, and humanitarian issues arise with lethal autonomous weapon systems. The possibility of international conventions that forbid the development of weapons judged to be tolerably dangerous is demonstrated by precedents such as the prohibition on chemical weapons. Autonomous weapons could make sense in a similar way.

In conclusion, The disruptive potential of AI calls for a re-examination of the core ideas that underpin international law. Regional dynamics could be destabilised by powerful algorithms under the direction of few individuals. Law must change to promote the advantages of AI while limiting its perils. Achieving effective governance will be pivotal as the technology radiates across the global

community.

1 https://ccdcoe.org/research/tallinn-manual/

2 https://hir.harvard.edu/establishing-cybersecurity-norms-in-the-united-nations-the-role-of-u-s-russia-divergence/

3 https://www.hrw.org/report/2020/08/10/stopping-killer-robots/country-positions-banning-fully-autonomous-wepons