



Artificial intelligence-driven terrorism as a crime against humanity: Normative gaps, legal frameworks, and the imperative of global governance reform

Aditya Vardhan¹, Dr. Jyoti Yadav^{2*}

¹ Amity Law School, Amity University Lucknow Campus, Lucknow, Uttar Pradesh, India

² Assistant Professor, Amity Law School, Amity University Lucknow Campus, Lucknow, Uttar Pradesh, India

Correspondence Author: Dr. Jyoti Yadav

Abstract

The convergence of artificial intelligence (AI) with extremist ideologies and terrorist operational methodologies represents one of the gravest threats confronting the international community in the twenty-first century. This paper undertakes an interdisciplinary examination of AI-driven terrorism — characterised by the deliberate weaponisation of AI technologies to plan, finance, recruit, execute, and propagandise acts of terrorism at unprecedented scale. Employing doctrinal legal analysis alongside comparative and case study methodologies, the paper analyses five principal modalities through which AI facilitates terrorism: autonomous weapons systems, AI-enabled cyberterrorism, deepfake and synthetic media deployment, AI-powered surveillance evasion, and algorithmic radicalisation. It critically assesses whether widespread, systematic AI-driven terrorist campaigns targeting civilian populations may constitute crimes against humanity under the Rome Statute of the International Criminal Court, and identifies fundamental lacunae in the existing international legal and governance architecture. The paper argues that the absence of a comprehensive international counter-terrorism convention specific to AI, combined with unresolved attribution challenges and jurisdictional limitations of the ICC, creates a dangerous governance vacuum. Drawing on comparative analysis of national responses from the United States, European Union, China, and India, the paper advances concrete recommendations including a binding UN Convention on Artificial Intelligence and Terrorism, the establishment of an AI-Terrorism Monitoring Agency, mandatory dual-use AI auditing, and the incorporation of AI ethics frameworks into counter-terrorism legislation. The paper concludes that anticipatory governance mechanisms, adequate to the accelerating pace of AI innovation, must be urgently developed before AI-driven terrorism transitions from an emerging risk into a systemic, civilisation-level threat.

Keywords: Artificial intelligence, terrorism, crime against humanity, international criminal law, autonomous weapons, deepfakes, cyberterrorism, AI governance, Rome statute, counter-terrorism

Introduction

The twenty-first century has witnessed an unprecedented convergence of two defining forces: the exponential advancement of artificial intelligence technologies and the persistent evolution of terrorism as a global security threat. Individually, each poses formidable challenges to states, international organisations, and civil society. Together, they constitute a paradigm-shifting threat matrix that the existing international legal, political, and technological order has yet to adequately address.

AI, broadly understood as the simulation of human cognitive processes by computational systems, has transformed virtually every sector of modern society — from healthcare and transportation to finance and law. Machine learning algorithms diagnose diseases, compose text in multiple languages, and navigate autonomous vehicles. Large language models generate contextually nuanced content with human-level fluency. Computer vision identifies faces in crowds with accuracy exceeding human performance. This 'fourth industrial revolution' is accelerating in ways that challenge the adaptive capacity of regulatory institutions^[1].

Simultaneously, terrorism continues to evolve in ideological form, organisational structure, and operational methodology. ISIS demonstrated how extremist organisations could exploit digital communications platforms to recruit globally and coordinate transnational operations. Right-wing extremist movements in Europe and

North America have likewise leveraged online ecosystems to propagate ideology and plan attacks. The intersection of AI and terrorism is not merely theoretical: drone attacks by non-state actors in Yemen and Ukraine, algorithmically accelerated radicalisation on social media platforms, deepfake disinformation campaigns inciting inter-communal violence in South Asia, and AI-enhanced cyberattacks on critical infrastructure are already documented realities.

The framing of AI-driven terrorism as a potential crime against humanity reflects the gravity and systemic character of the threat. Under Article 7 of the Rome Statute of the International Criminal Court, crimes against humanity encompass acts committed as part of a widespread or systematic attack directed against any civilian population, with knowledge of the attack^[2]. This paper argues that where AI systems are deliberately weaponised to conduct or facilitate mass violence against civilian populations in a systematic manner, the legal thresholds of crimes against humanity may be met, generating individual criminal responsibility under international law. Given the rapid democratisation of powerful AI tools — capabilities that required state-level resources a decade ago now run on consumer hardware — the urgency of this inquiry cannot be overstated.

Research Objectives and Methodology

This paper pursues the following principal research objectives: (i) to provide a conceptual taxonomy of AI-

driven terrorism distinguishing it from conventional and cyber-terrorism; (ii) to examine the principal modalities through which AI is weaponised for terrorist purposes; (iii) to analyse whether, and under what conditions, AI-driven terrorism may constitute a crime against humanity under the Rome Statute; (iv) to identify gaps in existing international legal and governance frameworks; and (v) to advance concrete, evidence-based recommendations for legal reform. The paper employs a qualitative, interdisciplinary research methodology drawing upon doctrinal legal analysis, comparative law, and case study analysis. Doctrinal legal analysis involves systematic examination of international treaties, UN Security Council resolutions, ICC judgments, and national legislation. Comparative analysis examines national responses in the United States, European Union, China, and India. Case study analysis draws on publicly available evidence of documented incidents of AI-enabled terrorist activity to ground the legal and policy analysis in operational reality. Primary sources are supplemented by secondary scholarship in international criminal law, AI governance, terrorism studies, and cybersecurity.

Conceptual Framework: Defining AI-Driven Terrorism

AI-driven terrorism may be defined as the deliberate design, development, deployment, or weaponisation of artificial intelligence systems, algorithms, or AI-generated content by individuals, groups, or organisations — acting for ideological, political, religious, or other extremist purposes — to plan, finance, facilitate, or execute acts of terrorism; to recruit, radicalise, or propagandise for terrorist organisations; or to conduct information operations designed to incite, intimidate, or coerce civilian populations or governments.

This definition encompasses both the direct use of AI as a weapon (for instance, an autonomous lethal drone) and the indirect use of AI as an enabling tool (for instance, AI-generated propaganda that radicalises individuals who subsequently commit attacks). It distinguishes AI-driven terrorism from conventional terrorism by the centrality of AI technologies in the operational chain; from cyberterrorism by the broader range of AI modalities involved beyond direct cyber intrusion; and from autonomous weapons use in armed conflict by the non-state-actor perpetrator and the civilian targeting intent characteristic of terrorism^[3].

Several dimensions define the distinctive character of AI-driven terrorism relative to conventional threats. First, scalability: AI systems can conduct attacks or information operations at a scale impossible for equivalent human operational infrastructure, enabling a small group to achieve impact previously requiring large organisational machinery. Second, speed: AI-driven operations can unfold at machine speed, exceeding the response capacity of human counterterrorism institutions. Third, personalisation: AI enables targeting of individual vulnerabilities — psychological, physical, and digital — with unprecedented precision. Fourth, attribution opacity: AI-mediated attack chains introduce novel attribution difficulties that complicate legal accountability. Fifth, global reach: AI-driven operations are inherently transnational, exploiting digital infrastructure that crosses jurisdictional boundaries and outpaces existing governance frameworks.

Principal Modalities of AI-Enabled Terrorism

1. Autonomous Weapons and Lethal AI Systems

The most directly lethal modality of AI-driven terrorism involves autonomous or semi-autonomous weapon systems capable of identifying and engaging targets without continuous human operator oversight. The Islamic State documented experimentation with commercial drones modified to carry explosive payloads from approximately 2016, demonstrating that commercially available unmanned aerial vehicles (UAVs) enhanced with AI navigation and basic targeting could serve as effective tactical weapon platforms accessible to non-state actors^[4]. The August 2018 drone assassination attempt against Venezuelan President Nicolás Maduro using DJI M600 drones loaded with C-4 explosive demonstrated the political targeting application of drone-based violence. More significantly, the Houthi movement's deployment of the Qasef-K2 loitering munition in Yemen — designed to autonomously navigate to a designated target area and engage targets identified by on-board sensors — represents a documented case of meaningful autonomous target engagement by a non-state actor.

The progression from manually controlled to semi-autonomous to increasingly autonomous weapon platforms among non-state actors is confirmed by multiple conflict monitoring organisations, including Conflict Armament Research and the UN Panel of Experts on Yemen. The combination of open-source AI navigation software, commercially available drone hardware, miniaturised explosive payloads, and reinforcement learning-based guidance creates a feasible near-term pathway to genuinely autonomous terrorist strike systems — systems whose operation may require no human involvement beyond initial programming and deployment.

2. AI-Enabled Cyberterrorism

AI dramatically enhances the capability, speed, and sophistication of cyberattacks against critical infrastructure, thereby expanding the potential for cyberterrorism — the use of digital attacks to cause fear, disruption, or harm to civilian populations and governments. AI-enhanced cyberattacks can automate vulnerability identification in target systems, generate and adapt malware in real time to evade detection, conduct distributed denial-of-service attacks at machine speed, and optimise phishing and social engineering campaigns with personalised targeting^[5].

The potential consequences for critical infrastructure — power grids, water treatment systems, financial networks, and hospital systems — are severe. A systematic AI-enhanced cyberattack campaign that incapacitates healthcare systems of a targeted population over an extended period, resulting in preventable deaths among vulnerable individuals who cannot access medical care, could, on the paper's analysis, constitute the sub-category of extermination as a crime against humanity under Article 7(2)(b) of the Rome Statute.

3. Deepfake and Synthetic Media

Generative AI systems — including generative adversarial networks (GANs) and diffusion models — can produce photorealistic synthetic audio, images, and video indistinguishable from genuine media. From a terrorist perspective, deepfakes present overlapping threat vectors: incitement of inter-communal violence through fabricated

evidence of atrocities; strategic political disinformation that triggers diplomatic crises or institutional responses; voice cloning to impersonate government officials or emergency services; and AI-generated text enabling coordinated information operations that manipulate public opinion^[6]. The 2022 deepfake video of Ukrainian President Zelensky appearing to order Ukrainian forces to surrender — while quickly debunked — demonstrated the operational deployment of synthetic media in conflict contexts. More sophisticated actors, operating with greater technical resources and longer planning horizons, could produce higher-quality synthetic media content capable of triggering real-world violence before detection and correction. AI-generated text at scale can also manipulate algorithmic content distribution systems, creating false impressions of widespread public support for extremist positions.

4. AI-Powered Surveillance Evasion

Paradoxically, the same AI capabilities that enhance state counter-terrorism surveillance simultaneously provide sophisticated tools for terrorist actors seeking to evade detection. Adversarial perturbation attacks — subtle modifications to physical appearance using specially patterned glasses, makeup, or clothing — can reliably defeat commercial facial recognition systems. AI-based voice modification systems can alter vocal characteristics to defeat voice recognition analysis. AI-based text style transfer can modify writing style to defeat authorship attribution. Network traffic analysis evasion tools can generate cover traffic patterns that conceal encrypted extremist communications^[7]. These capabilities are commercially available, originally developed for legitimate privacy protection, creating governance challenges analogous to those historically posed by dual-use encryption.

5. Algorithmic Radicalisation

Perhaps the most pervasive modality of AI-driven terrorism is algorithmic radicalisation: the process by which AI-powered content recommendation systems systematically expose individuals to progressively extreme content, accelerating radicalisation pathways. Content recommendation algorithms on platforms including YouTube, Facebook, and TikTok are optimised to maximise user engagement metrics. Research — including investigations by former platform engineers — has consistently demonstrated that emotionally provocative, boundary-pushing content generates higher engagement, causing recommendation algorithms to progressively expose users to more extreme material^[8].

Targeted advertising algorithms can be exploited by terrorist recruiters to deliver radicalisation content to psychologically susceptible individuals — those exhibiting social isolation, identity crisis, and susceptibility to conspiratorial thinking — with precision analogous to Cambridge Analytica's political micro-targeting. AI-powered chatbots fine-tuned on extremist ideology can simultaneously engage thousands of potential recruits in personalised, real-time conversations at near-zero marginal cost, representing a frontier application that current regulatory frameworks are wholly unprepared to address.

AI-Driven Terrorism and Crimes against Humanity: Legal Analysis

1. Article 7 Rome Statute Framework

Article 7 of the Rome Statute defines crimes against humanity as acts — including murder, extermination,

deportation, persecution, and other inhumane acts — committed as part of a widespread or systematic attack directed against any civilian population, with knowledge of the attack. An attack for these purposes is defined in Article 7(2)(a) as a course of conduct involving the multiple commission of specified acts pursuant to or in furtherance of a State or organisational policy.

AI-driven terrorism can, on the paper's analysis, satisfy each of these elements under specific conditions. The 'multiple commission' and 'policy' requirements are satisfied by a deliberate decision by a terrorist organisation to weaponise AI systems in a sustained campaign against civilian populations. The 'widespread or systematic' requirement — which is disjunctive, either element being sufficient — is met by AI's inherent scalability and the regularised, rule-governed character of algorithmic systems. An AI propaganda campaign systematically radicalising thousands of individuals across multiple countries, resulting in coordinated violent attacks, could be both widespread (in geographic reach and number of victims) and systematic (in its algorithmic, organised character). The 'directed against a civilian population' element is intrinsic to terrorism by definition.

2. Attribution and Accountability Challenges

The attribution of criminal responsibility in AI-mediated terrorism raises genuinely novel legal questions. The knowledge element of Article 7 — awareness that one's conduct is part of a widespread or systematic attack — is satisfied where an AI system is specifically designed and deployed for that purpose, but may be more difficult to establish where the AI system's harmful acts are an emergent consequence of its design. The ICC's mode of liability of 'perpetration by means' — which holds individuals criminally responsible for crimes committed through the instrumentalisation of others — offers a potential doctrinal pathway for attributing responsibility to those who deliberately deploy radicalisation algorithms to cause violence, though the application of this concept to AI-mediated causation chains has not been judicially tested^[9]. Command responsibility under Article 28 of the Rome Statute — holding superiors responsible for crimes committed by forces under their effective control where they knew or should have known of the crimes — has potential application to leaders of terrorist organisations that deploy AI systems, provided the requisite knowledge and failure to prevent or punish can be established. However, the AI responsibility gap — the absence of any natural person who made the ultimate decision to harm in cases of fully autonomous AI action — creates accountability lacunae that existing modes of liability were not designed to address.

3. Existing Framework Inadequacies

The existing international legal architecture is fundamentally inadequate for addressing AI-driven terrorism. The sixteen sectoral UN counter-terrorism conventions and protocols were designed for a pre-AI technological environment and do not contemplate the specific challenges of autonomous lethal systems, AI-generated propaganda, or algorithmic radicalisation. International humanitarian law, while applicable to armed conflicts involving AI systems, does not comprehensively address the use of AI by non-state terrorist actors outside armed conflict contexts. The Rome Statute framework, while potentially applicable, was not drafted with AI-mediated violence in mind^[10].

The emerging AI governance frameworks — including the EU Artificial Intelligence Act (2024), the UNESCO Recommendation on the Ethics of Artificial Intelligence, and the OECD AI Principles — represent significant achievements but remain inadequate for the terrorism dimension. The EU AI Act, the world's first comprehensive regulatory framework for AI, does not directly address the terrorist weaponisation of AI systems. International governance frameworks are predominantly voluntary, non-binding, and focused on commercial AI applications rather than security-specific dual-use scenarios. Regulatory arbitrage — the exploitation of jurisdictions with minimal AI oversight — enables terrorist actors to develop or deploy AI capabilities outside the reach of governance mechanisms.

Comparative National Responses

The paper analyses national responses in four representative jurisdictions to identify both governance progress and remaining gaps.

The United States has invested most substantially in AI counter-terrorism capabilities through its intelligence and defence apparatus, including the Joint Artificial Intelligence Center (JAIC) and subsequent integration into the Chief Digital and Artificial Intelligence Office (CDAO). The National Security Commission on Artificial Intelligence's 2021 Final Report identified AI as essential to national security. However, US counter-terrorism legislation does not specifically address AI-enabled terrorism, and the fragmented AI governance landscape across multiple federal agencies creates regulatory incoherence.

The European Union has enacted the most comprehensive AI governance framework with the AI Act (2024), employing a risk-based regulatory classification. While prohibiting certain high-risk AI applications and requiring conformity assessments for others, the Act does not specifically address AI weaponisation by terrorist actors or the international law dimensions of AI-enabled terrorist crimes. The Digital Services Act provides complementary obligations on very large online platforms regarding systemic risks from recommendation systems, representing meaningful progress on algorithmic radicalisation governance.

China's national AI strategy incorporates explicit counter-terrorism dimensions, with significant investment in AI-powered surveillance and content moderation for counter-terrorism purposes. China has proposed bilateral AI governance agreements and engaged in UN AI governance discussions, though its approach prioritises state security over individual privacy rights in ways that create human rights concerns. India's counter-terrorism legal framework — principally the Unlawful Activities (Prevention) Act — does not specifically address AI-enabled terrorism, though India's experience with drone-based cross-border terrorism has catalysed anti-drone investment and regulatory development, and India's participation in the Global Partnership on Artificial Intelligence and the Quad's Critical and Emerging Technologies Working Group provides multilateral governance engagement opportunities.

Recommendations for Reform

1. International Legal Reform

The most urgent priority is negotiation of a binding UN Convention on Artificial Intelligence and Terrorism, providing universal definitions of AI-driven terrorist acts,

establishing state obligations to criminalise AI-enabled terrorism under domestic law, creating a legal framework for attribution of AI-mediated terrorist acts, addressing jurisdictional challenges arising from the transnational nature of AI systems, and providing for extradition and mutual legal assistance in AI terrorism cases. As an interim measure, amendment of existing UN counter-terrorism conventions to explicitly encompass AI-enabled modalities, and adoption of a UN Security Council Resolution specifically addressing AI and terrorism, should be urgently pursued.

The Rome Statute should be supplemented with interpretive guidance — developed through the Assembly of States Parties — clarifying the application of Article 7 to AI-mediated violence: specifically addressing the knowledge requirement in cases of emergent AI behaviour, the application of command responsibility to AI system deployment decisions, and evidentiary standards for prosecuting AI-enabled terrorist crimes. The ICJ should be invited to render an advisory opinion on the application of existing international law to AI-enabled terrorist violence, providing authoritative guidance for states and international organisations.

2. Institutional Mechanisms

A dedicated AI and Terrorism Monitoring Centre, established under the auspices of the UN Counter-Terrorism Committee Executive Directorate, should be tasked with conducting annual threat assessments, monitoring convention implementation, providing technical assistance to developing countries, and coordinating the international response to AI terrorism incidents. A parallel AI Safety and Security Council — analogous to the IAEA's role in nuclear security — should develop and monitor compliance with international standards for AI systems with terrorism-enabling potential, with authority to conduct facility inspections and issue safety certifications. International intelligence sharing mechanisms should be expanded to include AI-specific threat intelligence, and a global database of AI-generated terrorist content — a deepfake equivalent of the Global Internet Forum to Counter Terrorism hash database — should be established for cross-platform identification and removal.

3. Technical Standards and Industry Obligations

Binding international technical standards for AI systems with terrorism-enabling potential should be developed through international standards bodies including ISO, IEC, and IEEE. Mandatory pre-deployment safety testing for AI systems above a specified capability threshold — with specific protocols for dual-use and terrorism-enabling applications conducted by accredited independent evaluators — should be incorporated into both international standards and national regulations. Content provenance standards — technical mechanisms for tracking the origin and modification history of AI-generated content, such as the C2PA (Coalition for Content Provenance and Authenticity) standard — should be made mandatory for AI-generated content published through major platforms. Major AI developers should be required to maintain explainable AI systems that generate audit trails usable as evidence in legal proceedings.

4. National Legislative Action

States should immediately audit their counter-terrorism legislation for gaps in coverage for AI-enabled modalities,

enacting targeted amendments to ensure that AI-assisted terrorist acts — programming and deploying autonomous attack systems, creating AI-generated incitement content, AI-enhanced targeting of critical infrastructure — are clearly covered by criminal offence provisions. National AI governance legislation should incorporate counter-terrorism dimensions including mandatory risk assessments for terrorism-enabling AI systems, restrictions on dual-use AI exports to jurisdictions with inadequate governance, and enhanced criminal penalties for deliberate AI weaponisation. Critical infrastructure protection legislation should require AI security assessments, AI-specific cybersecurity measures, and incident reporting obligations for AI-enabled attacks. India's existing legislative framework under the UAPA and IT Act should be expressly extended to encompass AI-enabled terrorist modalities, with the Drone Rules 2021 strengthened to include counter-terrorism AI requirements.

Conclusion

AI-driven terrorism is not a theoretical or futuristic concern; it is an emerging reality already visible in documented incidents of drone-based attacks by non-state actors, algorithmic propaganda operations, deepfake disinformation in conflict contexts, and AI-enhanced cyberattacks on critical infrastructure. The trajectory of AI capability development — characterised by exponential advancement, rapid democratisation, and progressive erosion of technical barriers to weaponisation — ensures that the threat will intensify significantly in the coming decade.

The paper has demonstrated that widespread, systematic AI-driven terrorist campaigns targeting civilian populations can satisfy the legal elements of crimes against humanity under Article 7 of the Rome Statute, subject to the resolution of novel attribution and accountability challenges. However, the existing international legal and governance framework — comprising pre-AI counter-terrorism conventions, voluntary AI governance frameworks, and ICC accountability mechanisms not designed for AI-mediated violence — is fundamentally inadequate to the challenge.

The governance agenda advanced in this paper — a binding UN Convention on Artificial Intelligence and Terrorism, dedicated international monitoring institutions, mandatory technical standards for dual-use AI, and national legislative reform — is calibrated to the scale of the threat while acknowledging institutional constraints on international legal reform. The ethical imperative of meaningful human control over consequential AI decisions, algorithmic accountability, non-discrimination, and proportionality must infuse every dimension of the counter-terrorism response to AI.

The international community stands at a pivotal moment. The decisions made in the next five to ten years about what AI systems are developed and deployed, by whom, under what constraints, and with what accountability will shape the AI landscape for decades. If those decisions are made without adequate attention to the terrorism-enabling potential of powerful AI, the consequences could be catastrophic and irreversible. Anticipatory governance — responsive not merely to threats that have already materialised but to those that are credibly foreseeable given the trajectory of AI capability development — is the defining governance imperative of our era.

Author Contributions: Aditya Vardhan conceptualised the study, conducted the literature review and legal analysis,

and drafted the manuscript. Dr. Jyoti Yadav supervised the research, provided critical scholarly guidance, and reviewed and revised the manuscript for intellectual content.

Conflict of Interest: The authors declare no conflict of interest.

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

References

- Schwab K. *The Fourth Industrial Revolution*. World Economic Forum, Geneva, 2016.
- Rome Statute of the International Criminal Court, July 17, 1998, 2187 U.N.T.S. 90, Art. 7.
- Brundage M, *et al.* *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Future of Humanity Institute Technical Report, Oxford, 2018.
- Conflict Armament Research. *Anatomy of the Islamic State's Drone Supply Chain*. Conflict Armament Research, London, 2017.
- Singer PW, Friedman A. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, 2014.
- Farid H. Fake News in the Age of AI. *Communications of the ACM*,2020;63(1):52-59.
- Payne K. Artificial Intelligence: A Revolution in Strategic Affairs? *Survival*,2018;60(5):7-32.
- Lewandowsky S, *et al.* Misinformation and Its Correction: Continued Influence and Successful Debiasing. *Psychological Science in the Public Interest*,2012;13(3):106-131.
- Prosecutor v. Katanga, Case No. ICC-01/04-01/07, Judgment pursuant to Article 74 of the Statute, ¶ 1395 (Int'l Crim. Ct. Mar. 7, 2014).
- S.C. Res. 1373 (Sept. 28, 2001); S.C. Res. 2396 (Dec. 21, 2017).
- Russell S. *Human Compatible: Artificial Intelligence and the Problem of Control*. Viking, 2019.
- Scharre P. *Army of None: Autonomous Weapons and the Future of War*. W.W. Norton, 2018.
- Roff H. The Meaningful Human Control of Autonomous Weapons Systems. *Artificial Intelligence & Society*,2014;29(1):1-17.
- Heyns C. Autonomous Weapons Systems: Living a Dignified Life and Dying a Dignified Death. In: Bhuta N, *et al.*, editors. *Autonomous Weapons Systems: Law, Ethics, Policy*. Cambridge University Press, 2016.
- European Parliament. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*, 2024.
- UNESCO. *Recommendation on the Ethics of Artificial Intelligence*. UNESCO, Paris, 2021.
- UN Secretary-General. *Our Common Agenda: Report of the Secretary-General*. United Nations, New York, 2021.
- Wing J. Trustworthy AI. *Communications of the ACM*,2021;13(4):64-71.
- Stern J, Berger JM. *ISIS: The State of Terror*. HarperCollins, 2015.
- Ohlin J. The Combatant's Privilege in Asymmetric and Covert Conflicts. *Yale Journal of International Law*,2015;40(2):337-392.