PRESENT

OUTCOME DOCUMENT

INTERNATIONAL CONFERENCE ON CYBERLAW, CYBERCRIME & CYBERSECURITY

12th Edition

Adopted by the Participants of the International Conference on Cyberlaw, Cybercrime & Cybersecurity (19–21 November 2025)

New Delhi, India

CONFERENCE THEME

Artificial Intelligence Ecosystem: Opportunities and Challenges

PREAMBLE

The Participants of the International Conference on Cyberlaw, Cybercrime & Cybersecurity (ICCC) 2025,

RECOGNIZING that artificial intelligence and emerging technologies are evolving at an unprecedented speed, similar to the development of humanity itself, and are fundamentally transforming socio-economic structures globally, governance paradigms, and relationships between human beings;

BUILDING ON the experience of 12 editions of this Conference, and recognizing that AI has moved from an experimental technology to a foundational infrastructure of the digital economy;

OBSERVING that the penetration of AI into critical sectors—healthcare, finance, defence, transport, and education—increases both transformative opportunities and systemic vulnerabilities that put individuals, institutions, and nations at risk;

NOTING that the accelerating technological landscape has decisively outrun current regulatory architectures and has created a compelling need for urgent harmonization of global AI governance frameworks, cybersecurity standards, and cybercrime enforcement mechanisms;

HIGHLIGHTING the existential threats created through algorithmic bias, deepfake technologies, autonomous cyberattacks, ransomware-as-a-service models, weaponized AI systems, and erosion of the truth in the digital information ecosystem;

APPRECIATING the collective contributions of policymakers, technologists, legal experts, civil society organizations, academic institutions, and industry stakeholders in improving multidisciplinary understanding and consensus building on the AI ecosystem;

AFFIRMING that trustworthy AI, secure digital infrastructures, ethical innovation, and equitable access are universal imperatives that require co-ordinated action across jurisdictions, sectors, and stakeholder communities;

UNDERLINING that generative AI, autonomous agents, and synthetic media are technologies with significantly increased ethical risks, which amplify misinformation campaigns, enable cognitive manipulations, and fundamentally challenge human autonomy, agency, and dignity;

TAKING NOTE that existing legal instruments on data protection, AI liability, intellectual property, and cybercrime remain insufficient to deal with critical gaps in transparency, explainability, accountability, and enforceability;

RECOGNIZING the profound challenges presented by Artificial General Intelligence, quantum computing capabilities, sophisticated supply-chain intrusions, and the convergence of biological and digital technologies, while acknowledging that coordinated national and multilateral preparedness can enable effective risk mitigation;

OBSERVING that synthetic and manipulated media erode public trust, compromise electoral integrity, violate intellectual property rights, and undermine the foundational institutions of democratic governance, and need comprehensive countermeasures;

EMPHASIZING that the absence of globally harmonized standards with regard to ethics in AI, privacy-by-design principles, Zero Trust security architectures, and human-centric technology development leaves critical national infrastructures dangerously exposed to escalating cyber threats;

NOTING that the dual-use nature inherent in AI enables both unprecedented innovation for human advancement and novel forms of discrimination, financial fraud, organized cybercrime, surveillance overreach, and autonomous weapons development;

REITERATING that strengthened international cooperation is indispensable in addressing the common transboundary challenges including drone warfare, blockchain regulation, cryptocurrency oversight, and post-quantum cryptography transitions;

AGREEING that it is necessary to have specialized forums that bring together educators, corporate leaders, investors, legal practitioners, and compliance officers for translating thought leadership, research insights, and best practices into actionable governance frameworks;

ANTICIPATING forward-looking approaches are sought to emerging concerns related to children's digital rights, Metaverse governance, neurotechnology ethics, the convergence of biotechnology and AI, and environmentally sustainable AI ecosystems.

DEMANDING effective legal remedies, institutional capacities, technical capabilities, and operational preparedness mechanisms to deal with AI-driven harms, systemic failures, and cascading risks;

COMMITTING to bridge the growing gap between technological acceleration and ethical, legal, regulatory, and policy oversight through inclusive dialogue, evidence-based policymaking, and adaptive governance;

CONFIRMING that the convergence of cyberlaw, cybersecurity, cybercrime prevention, and AI governance will profoundly shape global peace, security, economic prosperity, social cohesion, and sustainable development for generations to come.

CONFERENCE RESOLUTIONS

The International Conference on Cyberlaw Cybercrime & Cybersecurity 2025 resolved that:

1. Artificial intelligence is a transformative force hitherto unprecedented that will fundamentally reshape the ways in which humans think, economic forms, governance systems, human relationships, and even the path of human history itself.

2. The AI revolution brings an urgent imperative globally for a reevaluation by all stakeholders, including governments, private sector, civil society, academia, and international organizations, on policies, institutional frameworks, operational strategies, and ethical foundations with an unwavering emphasis on security, trust, equity, human rights, and sustainable development.

KEY RECOMMENDATIONS

A. LEGAL & REGULATORY EVOLUTION

The Participants call upon the International Conference on Cyberlaw, Cybercrime & Cybersecurity (ICCC) to:

1. Recognize Distinguished Leadership: Record formal appreciation for Dr. Pavan Duggal, Conference Director, who has provided outstanding strategic vision and thought leadership to further global discourse on AI governance, harmonization of cyberlaws, and emerging technology risks, besides creating an inclusive platform that pools together diverse stakeholders in pursuit of finding enduring solutions to most pressing digital challenges confronting humanity.

2. Strengthen Global Leadership: To continue to serve as the leading international platform that shapes legal scholarship, regulatory innovation, policy development, and best practices in the areas of cyberlaw, cybercrime prevention, cybersecurity, and AI governance.

3. Deepen Research Mandates: Substantially expand interdisciplinary research on the legal, ethical, societal, economic, political, and regulatory implications of AI and convergent technologies-IoT, blockchain, autonomous systems, quantum computing, neurotechnology, and biotechnology-AI integration.

4. Global AI Risk Taxonomy: Lead the formulation of a standardized, internationally interoperable classification framework for AI risks, including technical failures, misuse scenarios, cybercrime convergence, societal vulnerabilities, and existential threats, to drive regulatory coherence, early-warning detection systems, and cross-jurisdictional alignment.

5. Advancing Liability and Accountability Frameworks: Facilitate continued multi-stakeholder dialogue to address, in a holistic manner, AI liability attribution, algorithmic transparency requirements, explainability standards, bias detection and mitigation, fairness assessments, accountability for generative-AI-facilitated cybercrimes, and societal harms.

6. Safeguard the Digital Rights of Children: Develop binding, international standards that would protect young people from manipulative design, biometric surveillance, AI-powered behavioural profiling, microtargeted advertising, online exploitation, and developmental harms rooted in both the principles of privacy by default and age-appropriate design.

7. Advocate for Technological Foresight: Proactively address emerging and horizon-scanning concerns, including Zero Trust security architectures for IoT/5G/6G ecosystems, challenges in implementing post-quantum cryptography, the psychological and cognitive impacts brought about by AI, neurotechnology governance, ethics in brain-computer interface development, and the ever-evolving landscape of digital rights for vulnerable populations.

8. Organize Thematic Forums: Convene specialized global forums, expert working groups, and stakeholder consultations on the following topics: AGI governance frameworks; Metaverse

regulation; sustainable and climate-conscious AI models; advanced persistent threats; quantum-resistant cybersecurity; and biotechnology-AI convergence risks

9. Draft Metaverse Governance Frameworks: Lead in the drafting of wide-ranging regulatory schematics on digital property rights, avatar identity protection, virtual asset ownership, cross-platform interoperability, dispute resolution mechanisms, jurisdictional clarity, platform accountability, content moderation standards, and accessible redress pathways in case of harms experienced within virtual worlds.

10. Knowledge Infrastructure Creation: Create and publish focused knowledge resources, policy toolkits, legal templates, and technical guidance documents; deliver capacity-building programs to meet the needs of various stakeholders; and support large-scale public awareness on the aspects of cyberlaw, cybercrime prevention, digital literacy, and ethical deployment of AI.

11. Forge strategic alliances: Intensify partnerships with UN agencies, regional organizations, international law enforcement networks, standards bodies, academic consortia, and industry associations in the common quest to meet challenges posed by cyber warfare, drone threats, supply-chain compromises, critical infrastructure vulnerabilities, and emerging geopolitical cyber risks.

12. Lead on sustainable AI by actively advocating for energy-efficient AI model architectures, green data center infrastructures, mandatory carbon-impact disclosure requirements, circular economy principles relating to hardware, renewable-powered compute environments, and the integration of environmental sustainability considerations into AI governance frameworks aligned with global climate commitments.

13. Standardize AI Procurement: Develop detailed model procurement frameworks, contractual templates, and due diligence guidelines that articulate expectations of transparency, vendor accountability, risk allocation, security assurances, human rights impact assessments, interoperability standards, and ethical AI principles in both public and private sector procurements.

14. Support National Legislation: Provide expert technical assistance, policy guidance, legislative drafting support, and capacity-building resources to the states developing or updating AI legislation, data protection laws, cybercrime statutes, and digital rights frameworks that respect best international practices but also national contexts and constitutional traditions.

15. Strengthen Jurisprudential Development: Systematically monitor, document, analyze, and constructively influence the evolution of global cyberlaw precedents, AI governance frameworks, judicial interpretations, regulatory innovations, and international legal developments in a manner aimed at encouraging consistency, coherence, predictability, and justice in this digital century.

16. Expand stakeholder engagement through specialized roundtables, leadership summits, investor forums, CHRO and CISO convenings, academic partnerships, and civil society dialogues across different jurisdictions to foster serious cross-sector collaboration, knowledge sharing, building trust, and joint problem-solving on issues of mutual concern.

17. Map Generative AI Threats: Publish an authoritative annual global threat assessment that documents the trends, attack vectors, and emerging risks of AI-enabled cybercrime, including synthetic identity fraud, automated social engineering, AI-generated malware, algorithmic market manipulation, and deepfake-facilitated crimes that inform law enforcement strategies, regulatory responses, and defensive capabilities.

18. Create a Long-term Strategic Roadmap: Publish a comprehensive ten-year strategic vision document detailing concrete pathways, milestones, collaborative mechanisms, monitoring frameworks, and accountability measures to implement global AI governance, enhance cyber stability, and foster international peace and security, protect human rights, and achieve goals of sustainable development in a world transformed by AI.

B. HARMONIZED GLOBAL FRAMEWORKS

The Participants call upon the United Nations, its specialized agencies-including ITU, UNESCO, WIPO, UNDP, UNHCR-intergovernmental organizations, regional bodies, and civil society to:

1. Promote Global Harmonization: Foster common, interoperable, ethics-based, and human rights-based international AI governance frameworks that balance innovation with protection, economic development with equity, and technological progress with fundamental freedoms.

2. Institute Binding Standards of Accountability: Develop binding international norms, technical standards, and enforcement mechanisms on AI transparency, algorithmic explainability, accountability for automated decisions, and legal liability regarding deepfakes, facilitation of cybercrime, misuse of synthetic media, and AI-enabled human rights violations.

3. Enhance Global Response to Cybercrime: Significantly improve the level of international coordination in law enforcement, digital forensics, AI-enabled threat intelligence, ransomware response, cryptocurrency tracking, cross-border evidence sharing, extradition arrangements, and organizational resilience planning in order to prevent and respond effectively to transnational cybercrime networks.

4. Prohibit Fully Autonomous Weapons: Institute comprehensive, legally binding international treaties that would unmistakably prohibit the development, deployment, and use of lethal autonomous weapons systems devoid of meaningful human control and are integrated into disarmament agreements, humanitarian law frameworks, and peacekeeping protocols to maintain human agency and dignity in armed conflict.

5. Counter Synthetic Media: Establish and require global content provenance standards, cryptographic authentication systems, metadata transparency protocols, digital watermarking requirements, and accessible verification tools that help safeguard democratic integrity, media credibility, electoral processes, and the public's trust in the information ecosystem.

6. Advancing Cybersecurity Norms: Institute robust international standards, state responsibilities, confidence-building measures, and cooperative mechanisms to advance critical infrastructure resilience; supply-chain security assurance; coordination of vulnerability disclosure; incident response protocols; and common defence against AI-enabled warfare, zero-day exploits, and cascading cyber incidents.

7. Commission Research on Psychological Impacts: Support rigorous, multidisciplinary research examining the cognitive, behavioral, emotional, developmental, and societal effects of AI systems—including virtual companions, educational tutors, social media algorithms, decision-support tools, and persuasive technologies—to inform evidence-based safety guidelines, ethical standards, and mental health protections.

8. Safeguard Cognitive Liberty: Establish rigorous ethical and legal frameworks that expressly protect mental autonomy, freedom of thought, cognitive privacy, psychological integrity, and human agency from the growing AI-mediated environments in view, acknowledging that cognitive liberty is a basic human right entitled to protection by constitutional and international law.

9. Coordinate Global Efforts: Improve coherence, avoid duplication, and achieve maximum synergies among the current AI governance initiatives, standard-setting processes, regulatory experiments, and international dialogues by systematic information-sharing, joint action planning, harmonized timelines, and unified advocacy that accelerate collective progress on shared challenges.

10. Improved Cross-Border Governance: Building multilateral mechanisms, coordination platforms, and cooperation frameworks that can effectively respond to complex transnational challenges in drone warfare regulation, blockchain oversight, cryptocurrency governance, decentralized autonomous organization accountability, and post-quantum cryptographic standards transitions.

11. Lead Workforce Reskilling: Synchronize ambitious global skills development programs, just transition frameworks, lifelong learning initiatives, and social protection systems to support workers and communities affected by AI-driven automation, ensuring inclusive economic adaptation that preserves human dignity, and creates pathways to meaningful employment in the transformed labor market.

12. Ensure Effective Redress: Develop accessible, fair, efficient, and harmonized cross-border mechanisms-including specialized tribunals, ombudsperson offices, online dispute resolution platforms, and collective redress procedures-for investigating complaints, adjudicating

disputes, and providing meaningful remedies for AI-related harms, rights violations, and systemic injustices.

13. Promote Ethical Governance: Actively foster the formulation and sharing of common risk assessment methodologies, impact evaluation frameworks, ethical design principles, participatory models of governance, and best practices proven to align technological innovation with human values, imperatives of social justice, and sustainable development.

14. Design AI Dispute Resolution Mechanisms: Establish specialized arbitral frameworks, procedural rules, expert rosters, and institutional infrastructures that can efficiently adjudicate complex cross-border disputes arising from AI liability, provide predictable legal pathways, reduce jurisdictional uncertainty, boost business confidence, and protect consumer rights.

15. Regulate Humanitarian AI: Create comprehensive international norms, ethical directives, and mechanisms for ensuring accountability surrounding the utilization of AI technologies in humanitarian contexts-such as refugee status determination, disaster relief coordination, crisis prediction systems, and aid distribution-with human dignity, non-discrimination, transparency, safety, informed consent, and vulnerable population protection at the core.

16. Harmonize Blockchain Governance: Develop globally aligned regulatory frameworks, technical standards, and interoperability protocols for blockchain-based decentralized identity systems, smart contract enforceability, tokenized asset regulation, decentralized autonomous organization governance, and cross-chain transactions to enable secure innovation while preventing misuse, fraud, and systemic risks.

17. Publish Joint Ethical Guidelines: Through UN-Intergovernmental Organizations (IGO) collaboration, issue coordinated and authoritative ethical principles and operational guidance, underscoring the following basic reference standards as universally applicable to governments, corporations, and developers, including mandatory human oversight, proportionality assessments, comprehensive risk mitigation, algorithmic transparency, contestability rights, and accountability mechanisms.

18. Safeguard Electoral Integrity: Establish binding international standards, cooperative enforcement mechanisms, transparency obligations, and rapid response protocols to help prevent and counter AI-enabled electoral manipulation, microtargeted voter suppression, automated disinformation campaigns, synthetic candidate impersonation, algorithmic opinion manipulation, and information warfare that threatens the core of democratic self-governance.

19. Clarify IP Rights for AI-Generated Works: Support WIPO-led international harmonization efforts towards developing coherent, balanced IP frameworks governing authorship attribution, determination of ownership, licensing regimes, moral rights, and equitable

benefit sharing for AI-created creative works, balancing innovation incentives with creator protection and public interest considerations.

20. Address AGI and Existential Risks: Recognize the unparalleled challenges and potentially disastrous risks of AGI development, advanced AI systems surpassing human cognitive capabilities, and quantum computing breakthroughs; establish special international coordination mechanisms, early warning systems, containment protocols, and emergency response frameworks for the efficient assessment, mitigation, and governance of risks.

21. Inclusion and Equity: AI systems, policies, and governing frameworks should actively promote fairness, access, non-discrimination, cultural sensitivity, and equity for all communities, with particular attention to the needs of women, children, elderly persons, persons with disabilities, indigenous peoples, racial and ethnic minorities, refugees, and other historically marginalized populations.

22. Create an International AI Ombudsperson: Establish an independent, adequately resourced, globally accessible oversight institution empowered to receive individual and collective complaints, conduct impartial investigations, document patterns of AI-related abuses and rights violations, recommend corrective actions and policy reforms, and report publicly on systemic issues requiring international attention and remedy.

23. Make reporting at the nation-state level mandatory: Invite member states to provide detailed annual or biennial reports on AI risk assessments, significant incident reports, mitigation strategy updates, descriptions of governance frameworks, and lessons-learned analyses in one easily accessible UN registry for encouraging shared learning; guaranteeing transparency; global situational awareness; enabling comparative cross-country analysis; and informing evidence-based governance reforms and technical assistance programs.

24. Publish AI Harmonization Index: Create and publish an authoritative annual benchmarking index that transparently measures and ranks national alignment to global standards on AI, ethical guidelines, best practices in governance, commitment to human rights, and regulatory maturity indicators that will promote healthy international cooperation, provide capacity-building priorities, recognize leadership, offer opportunities for improvement, and become a guide for states on how to strengthen their AI governance ecosystems.

C. NATIONAL & STAKEHOLDER ACTION

The Participants call on national governments, legislative bodies, judicial institutions, educational systems, research organizations, professional associations, media institutions, civil society organizations, private sector entities, and all relevant stakeholders to:

1. Put in Place Comprehensive AI Legislation: Implement clear, enforceable, rights-respecting legal frameworks that establish governance obligations, safety requirements, risk management standards, accountability structures, transparency mandates, oversight

mechanisms, and accessible enforcement tools for AI systems, particularly for high-risk applications affecting fundamental rights, public safety, democratic processes, and critical infrastructure.

2. Criminalize Malicious AI Use: Provide specific criminal penalties, enhanced sentencing provisions, asset forfeiture mechanisms, and an international framework for cooperation in cases involving malicious AI deployment in terrorism, organized cybercrime, child exploitation, fraud, election interference, critical infrastructure attacks, and ransomware-as-a-service operations, ensuring that our legal tools keep pace with evolving threats.

3. Adopt Anticipatory Regulation: Institute prospective, adaptive regulatory approaches through techniques like horizon scanning methodologies, scenario planning exercises, technology foresight, regulatory sandboxes, experimental governance, periodic review cycles, and sunset provisions to proactively address emerging AI capabilities before their widespread deployment results in irreparable harm, thereby reducing regulatory lag and preventing societal damage that could otherwise be avoided.

4. Develop and clearly establish liability principles through the creation of comprehensive legal frameworks, judicial guidance, and precedent-setting cases on the allocation of liability, standards for causation, burden of proof, damage assessment methodologies, and mechanisms of remedy for AI-caused harms to individuals, communities, and society that will balance innovation incentives with robust victim protection and effective deterrence of negligent development and deployment.

5. Effectively Counter Disinformation: Establish multi-layered legal, technical, educational, and institutional frameworks to reduce AI hallucination-related risks, prevent the generation of synthetic media for malicious purposes, fight coordinated inauthentic behavior, increase platform accountability, strengthen quality journalism, and tackle Darknet-enabled disinformation operations, while ensuring freedom of expression and promoting media pluralism.

6. Invest Heavily in Education: Systematically integrate AI literacy, cyberlaw fundamentals, cybersecurity awareness, digital citizenship, computational thinking, data literacy, ethical reasoning, and critical evaluation skills into the curricula at all educational levels-from primary schools through universities and continuing professional development-building broad societal capacity to understand, question, participate in, and constructively shape AI-transformed societies.

7. Monitor Illicit Networks: Using advanced AI-powered monitoring systems, threat intelligence platforms, behavioral analysis tools, and international coordination mechanisms to detect and disrupt Darknet criminal activities including exploit trading, synthetic malware distribution, illicit AI model trafficking, ransomware marketplaces, and emerging cyber threats, with oversight and accountability conditions focused on protection of civil liberties in surveillance activities.

8. Define Stakeholder Responsibilities: Clearly stipulate the rights, duties, ethical obligations, liability exposures, and accountability mechanisms of each party in AI value chains, from developers to deployers, data providers, infrastructure operators, investors, regulators, users, and affected communities. This would bring about shared understanding of responsibilities and allow for effective governance by distributed accountability.

9. Protect National Sovereignty: Acknowledge and address the AI technology's capacity to undermine national sovereignty, territorial integrity, interfere with domestic affairs, facilitate foreign surveillance, enable hidden influence operations, and concentrate power at the expense of self-determination; establish proper technological, legal, diplomatic, and security safeguards while remaining open to salutary international cooperation.

10. Categorization of AI-Enabled Crimes: Officially acknowledge AI-facilitated criminal activities as specific classes that necessitate specially designed investigation techniques, forensic capabilities, prosecutorial expertise, judicial training, evidentiary standards, and sentencing frameworks combined with a coordinated prevention approach considering the peculiar technical nature, cross-border aspect, and dynamic modus operandi of AI-enabled crime.

11. Protect the Right to Privacy: Thoroughly examine the use of AI in light of personal data privacy, informational self-determination, surveillance capabilities, predictive profiling, behavioural monitoring, and autonomy. Provide strong legal safeguards against AI-facilitated privacy violations and the gradual expansion of surveillance through purpose limitation, data minimization, consent requirements, deletion rights, algorithmic transparency, and strict enforcement.

12. Incorporate AI Ethics Education: Provide culturally and age-sensitive education in AI ethics, algorithmic fairness, bias recognition, digital rights, privacy protection, and cybersecurity basics throughout systems of education, professional training, and public awareness campaigns as a means of developing knowledgeable, responsible, critical, and active digital citizens who can contribute significantly to the development and shaping of AI governance while holding powerful actors accountable.

13. Implement Binding Ethical Standards: Implement and strictly enforce robust ethical codes, professional standards, certification requirements, and accountability frameworks for AI development and deployment by both the public and private sectors, making abstract principles such as fairness, non-discrimination, explainability, contestability, proportionality, and human oversight concrete, measurable, auditable, and legally enforceable rather than aspirational statements.

14. Enhance Data Governance: Put in place consent-based, purpose-limited, and transparent data governance frameworks that establish clear rules, oversight mechanisms, and enforcement procedures governing how personal data is collected, processed, stored, shared, and used in training AI, with meaningful individual control, preventing function creep, and

mandating data minimization and anonymization where possible, protecting collective data rights and community interests.

15. Mandate Corporate Accountability: Organizations deploying high-risk AI systems should be compelled to operate under rigorous, routine compliance audits by competent, independent auditors utilizing harmonized frameworks for assessment; complete reporting of findings; public disclosure of material risk; meaningful consequences, including but not limited to very significant financial penalties and operational constraints for negligent or reckless deployment; and monitoring for continued compliance and sustained safety.

16. Make AI Transparent: Legislate that automated systems making or significantly impacting decisions affecting individual rights, opportunities, services, or freedoms be legally bound to clearly disclose the involvement of AI, provide accessible explanations of the processes and factors at play in their decision-making, offer meaningful opportunities for human review and appeal of those decisions, and provide accessible channels through which affected individuals can seek information, challenge decisions, and obtain redress when automated systems cause harm or perpetuate injustice.

17. Support Workforce Transition: Through adequately funded and effectively administered dedicated programs, displaced workers have access to comprehensive reskilling opportunities, career counseling, job placement assistance, income support during transitions, recognition of prior learning, portable benefits, regional economic development initiatives, and pathways to quality employment in emerging sectors to ensure AI's gains are shared broadly without deepening economic disruption, inequality, or social fragmentation.

18. Protect Critical Infrastructure: Mandate implementation of Zero Trust security architectures, continuous authentication protocols, network segmentation, least-privilege access controls, and AI-enabled anomaly detection systems across national critical infrastructure sectors-including energy, water, transportation, healthcare, finance, and communications-with regular security assessments, incident response planning, information sharing, and coordinated defense strategies to reduce systemic vulnerabilities and improve resilience against sophisticated cyberattacks.

19. Secure AI Supply Chains: Implement thorough Software Bills of Materials, firmware transparency, verification of hardware components, and supply chain risk assessments for AI systems to provide visibility into code origins, third-party dependencies, known vulnerabilities, and possible compromise vectors that enable informed procurement decisions, rapid vulnerability patching, mitigation of supply chain attacks, and limited exposure to embedded malicious elements and unexpected system behaviours.

20. Foster Multi-Stakeholder Dialogue: Through permanent national forums, advisory councils, public consultation processes, and participatory governance mechanisms, promote the regular and structured dialogues among government agencies, academic researchers, industry leaders, civil society advocates, affected communities, and technical experts to

enable collective problem-solving, harmonize policy approaches, share research findings, build trust, incorporate diverse perspectives, and strengthen inclusive, legitimate, effective AI governance ecosystems responsive to the evolving challenges.

21. Proper Training of Law Enforcement: Ensure the imparting of comprehensive, regular, rights-preserving training on the use of AI tools responsibly by police, prosecutors, judges, and forensic teams in investigation, evidence collection, analysis, and courtroom presentation, to ensure accuracy, reliability, fairness, and effectiveness, and setting up strong oversight systems, clear use policies, external auditing, and mechanisms of accountability that avoid misuse, function creep, discriminatory application, and infringement of rights, as well as unjustified mass surveillance, which undermines civil liberties and erodes public trust.

22. Implement AI Export Controls: Modernize and harmonize national export control legislation, licensing processes, and multilateral coordination mechanisms to cover appropriately calibrated, risk-based restrictions on sensitive AI models, dual-use systems, advanced training algorithms, large-scale compute clusters, specialized chips, and strategic technologies that pose threats to national security, human rights, or proliferation, underpinned by robust monitoring of compliance, effective enforcement, and frequent policy reviews to ensure that controls remain effective, proportionate, and enabling of innovation.

23. Establish Regulatory Sandboxes: Well-designed regulatory sandbox environments, innovation testbeds, and controlled experimentation zones should be established that allow responsible innovators to test novel AI systems, business models, and approaches to governance under active regulatory supervision, real-world conditions, and enhanced monitoring whereby regulators can systematically observe risk factors, gather evidence, learn from experience, and iteratively develop informed policy in support of beneficial innovation, management of public safety risks, and enabling responsible market entry.

24. Advance Media Literacy: Develop and implement comprehensive, well-resourced national campaigns on media literacy, education, public toolkits, community workshops, and digital citizenship to provide citizens-especially the young, elderly, and vulnerable-with critical source evaluation, deepfakes and manipulated content identification, misinformation pattern recognition, algorithmic curation understanding, and methods of resistance against AI-enabled manipulation that will enhance individual resilience, democratic engagement, and societal capacity for shared epistemic foundations; this is required for collective decision-making.

25. Mandate Environmental Standards: Require data centers, cloud computing providers, AI training facilities, and compute clusters to meet ambitious green energy benchmarks, energy efficiency standards, water conservation targets, and comprehensive sustainability reporting obligations; incentivize renewable energy adoption, waste heat recovery, circular hardware practices, and responsible e-waste management that would substantially reduce the growing

carbon footprint of AI, its water use, and environmental impacts, while aligning technological progress with urgent climate goals and planetary boundaries.

26. Fund AI Safety Research: Long-term, sufficient, unconditional public funding for independent, interdisciplinary AI safety research across computer science, law, ethics, psychology, economics, political science, sociology, and behavioral sciences should be given, including technical alignment research, robustness testing, interpretability methods, fairness metrics, governance experiments, and impact studies. Research output should systematically feed into informed policy-making, industry standards, education, and the public through easily accessible publication and active dissemination.

27. Incentivize Responsible Innovation: Targeted grants, tax incentives, preferential procurement, regulatory fast-tracks, incubation programs, mentorship networks, and market access support given to startups, researchers, and organizations developing ethical, safety-oriented, socially beneficial, environmentally sustainable, accessibility-focused, and human-rights-respecting AI technologies and applications will strengthen national innovation ecosystems, foster responsible entrepreneurship, create quality jobs, enhance international competitiveness, and make sure technological progress serves broad public interests rather than narrow commercial gain.

28. Require Transparency Reporting: Require large technology companies, public sector organizations, and high-risk AI deployers to publish comprehensive annual AI accountability reports transparently that outline the systems deployed, risks assessed, incidents documented, the safeguards implemented, mitigation measures, governance structures, stakeholder engagement, impact assessments, future plans, and lessons learned; with meaningful penalties-including fines, operational restrictions, reputational consequences-for nondisclosure, incomplete reporting, or deliberate obfuscation to build trust with the general public, enable scrutiny from informed actors, underpin regulatory oversight, and create incentives for continuous improvement.

29. The National AI Safety Boards should be well-resourced, politically independent, with statutory authority, technical expertise, investigatory powers, and public accountability mandates to investigate systematically significant AI-related accidents, near-misses, systemic vulnerabilities, pattern failures, and emerging risks via rigorous root cause analysis; publish findings, evidence-based recommendations, and regulatory guidance for evolving national standards, industry best practices, and educational programs; develop risk mitigation policies to build institutional knowledge and public confidence.

30. Monitor Emerging Synthetic Threats: Establish national-level threat observatories, early-warning centers, or specialized intelligence units with leading technical capacities that can continually map, analyze, and disseminate actionable intelligence on emerging synthetic threats, including-but not limited to-autonomous malware evolution, generative AI attack vectors, adversarial machine learning exploitation, biotechnology-AI convergence risks,

quantum computing implications, and novel cyber-physical vulnerabilities-through periodic unclassified risk bulletins, allowing for quick coordination between security agencies, critical infrastructure operators, private sector AI laboratories, and international partners.

31. Regulate Biometric Systems: Develop strict comprehensive legal frameworks to regulate the development, sale, deployment, and use of biometric AI systems including facial recognition, gait analysis, voice identification, emotion detection, and behavioural profiling that impose strict limits on indiscriminate mass surveillance; independent third-party accuracy and bias audits are to be required, especially for vulnerable groups; rigorous proportionality assessments and judicial authorization before any deployment in public spaces are to be implemented; clear retention limits and deletion requirements established; meaningful transparency provided about system capabilities and limitations; accessible redress mechanisms created for harms; and granting enforcement capabilities for regulatory authorities to investigate and sanction.

CALL TO ACTION

The Participants of the International Conference on Cyberlaw, Cybercrime & Cybersecurity 2025:

URGENTLY CALL FOR immediate, ambitious, coordinated international action to strengthen and harmonize global cyberlaw frameworks, align AI governance standards across jurisdictions, share proven best practices and lessons learned, and collectively implement comprehensive safeguards ensuring an AI-driven digital ecosystem that is fundamentally secure, operationally resilient, socially equitable, environmentally sustainable, rights-respecting, and genuinely conducive to inclusive economic development, human flourishing, democratic stability, and shared prosperity for all peoples and nations;

Solemnly urge all stakeholders to be constantly vigilant, exercise responsible stewardship, show proactive diligence, and embrace adaptive learning throughout this era of profound, rapid, and irreversible digital transformation-particularly in protecting critical information infrastructure, safeguarding democratic institutions, implementing Zero Trust security principles for converging IoT/5G/6G ecosystems, addressing the unique vulnerabilities of emerging technologies, countering sophisticated cyber threats, and steadfastly advancing responsible, ethical, transparent, accountable, sustainable and human-centered development and deployment of artificial intelligence and information and communication technologies;

EMPHATICALLY EMPHASIZE that the policy choices, regulatory frameworks, investment decisions, ethical commitments, and governance structures that are made in this critical moment will determine-in many cases, irreversibly-whether artificial intelligence develops into humanity's most powerful tool for solving global problems, enhancing human capabilities, mitigating suffering, and creating a more just and thriving civilization-or,

alternatively, into a dangerous accelerant of inequality, surveillance, manipulation, conflict, environmental destruction, and systemic vulnerability that undercuts human agency, dignity, and security, as well as the very bases of free, democratic, and peaceful societies.

ADOPTION

The Participants of the International Conference on Cyberlaw, Cybercrime & Cybersecurity hereby formally approve and adopt this Outcome Document.

Adopted: 21 November 2025

Location: New Delhi, India