INTERNATIONAL CONFERENCE ON CYBERLAW, CYBERCRIME & CYBERSECURITY

OUTCOME DOCUMENT *of the*

INTERNATIONAL CONFERENCE ON CYBERLAW, CYBERCRIME & CYBERSECURITY

ADOPTED BY THE PARTICIPANTS OF THE INTERNATIONAL CONFERENCE ON CYBERLAW, CYBERCRIME & CYBERSECURITY IN CYBERSPACE

(23RD TO 25TH NOVEMBER, 2022)

Supported By

Media Partner

Indian Infrastructure

nixi Empowering Netizens

Cyber Security Partner

paloalto NETWORKS

DELL Technologies

MARUTI SUZUKI Way of Life!

Autobot Infosec

विधि कार्य विभाग
DEPARTMENT OF LEGAL AFFAIRS

Ministry of Electronics and Information Technology
Government of India

University for Peace

UNITED NATIONS UNIVERSITY
UNU-EGOV

विज्ञान एवं प्रौद्योगिकी विभाग
DEPARTMENT OF SCIENCE & TECHNOLOGY

Ministry of Environment, Forest and Climate Change

Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

MEDIC

asia cloud computing association

ICCSL

Ecommerce Forum Africa

Globethics.net

Cyber Peace Foundation

IEEE TEMS
Technology & Engineering Management Society

Artificial Intelligence Law Hub

The Hague Centre for Strategic Studies

Cybersecurity-You

Cyberlaw University

Metavers Law Nucleus

International Conference on Cyberlaw, Cybercrime & Cybersecurity

PREAMBLE

UNDERSTANDING that the newly emerging technologies cannot be left unregulated;

REITERATING that in the time to come, technological advancements are source for worry and tools to help in the propagation of crimes and offences in the cyberspace;

AGREEING that law and technology sectors can no longer be exclusive;

ACCEPTING that it is time for judges, lawyers, law-makers, politicians and digital stakeholders to take note of the increasing technological advances;

RESTATING that the legal jurisprudence of yesteryears is no more relevant, in face of technology that is advancing with the speed of light;

WITNESSING the safety features like mobile passwords, PINs and other security features slowing becoming outdated, with the law still not developed to regulate these changes;

UNDERLINING that there needs to be separate legal provisions for protecting the Critical Information Infrastructure of each nation, due to the important role played by it;

ACKNOWLEDGING that already, a major part of wars in the physical world are actually being fought in the cyberspace;

NOTICING that the best way to paralyze a country is by paralyzing its Critical Information Infrastructure, with the method and mode of attack, being the most efficient tactic in the hands of external and internal malicious actors;

International Conference on Cyberlaw, Cybercrime & Cybersecurity

SPOTING that the laxity of cybercrime regulatory regimes have contributed to emergence of new kinds of cybercrimes;

NOTICING that Covid-19 has accelerated the growth of cybercrime, ushering in the potentially decades long Golden Age of Cybercrime;

UNDERSTANDING that the problem of Internet jurisdiction in bringing cybercriminals to justice can be solved only by mutual understanding and resolve at the international level;

APPRECIATING the efforts of individual governments that have started emerging to counter cybercrime;

FOCUSSING that cybersecurity is an often neglected area, which is not given the deserved attention;

UNDERSTANDING that although the cybersecurity landscape is still evolving, malicious actors have already started to pry into its vulnerabilities;

ACCEPTING that barring a few developed nations, most governments need to work on cybersecurity law, with specific legal provisions pertaining to cybersecurity being an absolute must for every jurisdiction;

FOCUSSING on how the private sector as well as the public sector are susceptible to constant menace of cyber security breaches;

EMPHASIZING that Ransomware has emerged as the foremost challenge in cyberspace for state and non-state actors;

REPEATING that specific and express legal provisions are required to deal with the use of Ransomware in the laws of every country;

ACKNOWLEDGING how Blockchain has emerged as a technology that is unprecedented in its effects;

UNDERSTANDING that since many new technical phenomena are based on Blockchain, there is a need for the evolution of specific laws on the same in each country;

REALIZING the importance of Web 3.0 and how its emergence has the power to bring more users on the Internet bandwagon;

NOTICING how the increased usage of the Internet will further lead to the abundant availability of data that is ready to be exploited;

STUDING how edge computing can have after effects which are not regulated by any law;

FOCUSING on the role played by social media in today's world and how many countries are doing too little too late in regulating social media;

NOTING the different type of cyber compliances needed to ensure that body corporates remain safe from cyber attacks, cyber breaches, data breaches;

UNDERSTANDING how mobile apps are gaining importance from a legal point of view, with the majority of malicious cyber actors orchestrating their attacks through mobile apps;

LOOKING at the emergence of fake news and how malicious actors spreading fake news gaslight the normal people into believing such stories;

TAKING into account innovative methods of coming up with solutions to regulate quantum computing, the emergence and practical impacts of which threatens to make passwords a futile exercise;

SEEKING to need to regulate OTT Platforms and how the content on such platforms can be brought more in line with the accepted morals of any society;

STUDING the psychological impacts of cyber bullying and why cyber bullying is gaining growing prominence in the cyberspace;

ATTEMPTING at creating the need for a set of generally accepted principles towards the activities of Public-Private Partnerships in cyberspace.

KEY RECOMMENDATIONS

THE PARTICIPANTS OF THE INTERNATIONAL CONFERENCE ON CYBERLAW, CYBERCRIME AND CYBERSECURITY HEREBY CALL UPON THE *INTERNATIONAL CONFERENCE ON CYBERLAW, CYBERCRIME AND CYBERSECURITY*

1. To continue working on various and evolving cutting-edge areas of cyberspace and their intersection with law and technology;

2. To specifically explore the cyber legal, cybercriminal and cyber security repercussions of emerging technologies like Artificial Intelligence, Blockchain, Internet of Things, Metaverse and Quantum Computing;

3. To come up with a separate smaller conference outside of India as a buildup event into the main conference;

4. To work on new challenges impacting the intersection of cybersecurity and law as also connected legalities and policy aspects;

5. To connect and interact with other stakeholders at the international level so as to understand their respective works in the areas of the intersection of Cyberlaw, Cybercrime and Cybersecurity and to collaborate with them on areas of mutual interest, value addition and knowledge enhancement;

6. To disseminate the recommendations of the conference to all stakeholders in the digital ecosystem across the world including governments, ministries, agencies, corporates, not for profits, international organizations and every stakeholder in their respective national jurisdictions who is either connected, associated or dealing with the aspects of cyberspace as also Cyberlaw, Cybercrime and Cybersecurity;

7. To work with digital stakeholders in a post-Covid scenario to identify, discuss, elaborate, analyze and also examine the newly evolving areas on the intersection of Cyberlaw, Cybercrime and Cybersecurity;

8. To contribute to enhanced capacity building by partnering up with appropriate partners in the direction of creating more capacities amongst all digital stakeholders;

9. To work with prominent industry leaders, thought leaders, experts and the stakeholders in different parts of the world on the thrust areas of the Conference;

10. To understand and appreciate the cutting edge developments in cyberspace, partner with other like-minded digital stakeholders, and to disseminate more knowledge, awareness,

information and capacities amongst various digital stakeholders in different parts of the world;

11. To examine the cyberspace ecosystem and emerging challenges in the context of the world post Covid-19 and explore the emerging trends, aspects, issues pertaining to cyberspace and to study and analyze the emerging jurisprudence concerning emerging technological paradigms in different parts of the world and try to collate common legal principles concerning the same;

12. To work on cutting edge developments in cyberspace including Metaverse, Quantum Computing, Internet of Things, Internet of Behaviour, Blockchain and Artificial Intelligence amongst other various disciplines so as to identify key emerging trends in emerging technologies, which could have a direct relevance and bearing upon the day to day operations and business activities of all digital stakeholders;

13. To become a catalyst for discussions on the key aspects of Cyberspace, and its future trends and impact, including legal, ethical, social, policy and regulatory issues thereof and present an integrated, holistic and strategic view of the issues therein, whilst recognizing that there is an urgent need for effective global cooperation on cyber issues amongst all stakeholders;

14. To network, interact, collaborate and work with global stakeholders on various aspects pertaining to activities in the digital ecosystem which would have a nexus, connection or association of any kind whatsoever with the connected paradigms of Cyberlaw, Cybercrime and Cybersecurity;

15. To identify the distinctive legal, policy, regulatory and technical challenges, issues and nuances thrown up by growing cyber security breaches and the potential approaches being adopted in this regard to deal with the menace of increasing cyber security breaches;

16. To identify and collate emerging international best practices that are evolving in different parts of the world on how fresh approaches need to be adopted, for dealing with the growing Golden Age of Cybercrime;

17. To clearly define 'Duty of Care' in the digital ecosystem for responsible governance;

18. To identify as to how cyberattacks can negatively affect cyber sovereignty, and related concerns of protecting cyber sovereignty of a nation;

19. To collaborate and develop approaches on how to reach on an agreement on acceptable cybersecurity norms respecting the principles enshrined in the United Nation Charter and promote a secure and stable cyberspace;

20. To highlight the gaps, challenges and vulnerabilities arising due the advances in Artificial Intelligence and solutions to remedy the risks of the AI system, and to deliberate upon the potential of AI in ensuring governance;

21. To highlight the issue of protection of individual rights behind the huge potential of Big Data and to ensure that the benefits of Big Data are shared equitably with sufficient transparency and accountability;

22. To collaborate with various international, national, and regional stakeholders to work together on the issue of anonymity in cryptocurrencies, the related technical and legal challenges and development of appropriate regulatory framework regarding the crypto ecosystem;

23. To reach out to connected stakeholders in the Cyberlaw domain at global, regional and national levels so as to keep a track of the latest evolving trends, issues and aspects in cyber legal jurisprudence and to further see how national Cyberlaw approaches are increasingly

being moulded to make them topical and relevant to latest technologies, with the passage of time;

24. To work on the intricate nuances of newly emerging cyber-ground realities post Covid-19 and how to deal with various the challenges thrown up by newly changed scenario of Cyberlaw, Cybercrime and Cybersecurity.

25. To study, examine and analyze the aspects of the new cyberage that governs the world post-Covid 19 and to identify key challenges and parameters for all stakeholders in this regard;

26. To explore the emerging trends concerning cyber-sovereignty and the various international legal challenges that the growing advent and consolidation of the concept of cyber-sovereignty is beginning to throw up for all digital ecosystem stakeholders as well to examine, from a global standpoint, the emerging phenomenon of balkanization of the internet and the connected legal policy issues connected therewith;

27. To explore how the misuse of the Darknet for criminal purposes can be appropriately addressed by State actors over the passage of time and to explore how the principles of attribution of cyber-acts done by cyber-actors can be further effectively evolved;

28. To come up with emerging cyber legal issues and challenges, post the commencement of the Ukraine War and their impact upon the global cyber ecosystem;

29. To encourage the adoption of more cyber resilient tools for digital stakeholders in view of the increased adoption of internet by all digital stakeholders and to promote effective information exchange for enhanced international cooperation on matters relating to cybercrime;

30. To study and explore along with the stakeholders on how cogent and effective steps can be taken to protect the privacy of users in the digital ecosystem and to disseminate awareness about the interconnected paradigms of Cyberlaw, Cybercrime and Cybersecurity and to inspire discussions at national, regional and international echelons on the intersection of Cyberlaw, Cybercrime and Cybersecurity to meet the complex challenges by focusing on achieving a secure, robust and resilient cyberspace;

31. To collate and interact with all international, regional and national projects and initiatives, programs and schemes which are being implemented having a direct impact upon the interconnected paradigm of Cyberlaw, Cybercrime and Cybersecurity;

32. To foster more discussions, dialogues and exchange of ideas, perspectives and opinions on the growing cyber legal challenges to the cyberspace ecosystem thrown up by various emerging paradigm;

33. To contribute to continuing international discussions upon evolving norms of behaviour regarding cyber operations;

34. To provide strategic leadership across Governments to respond to cyber security threats against identified Critical Information Infrastructure (CII);

35. To explore and analyse the various regional and national legislations on data protection and privacy and their contribution to strengthening the secure digital environment

36. To work towards decentralized data transparency, and legal foundations for peer-to-peer currency exchange, smart programmable contracts and for regulating crypto assets;

37. To identify and highlight the legal nuances and challenges raised by fake news globally and encourage the crystallization of appropriate legal response to deal therewith.

International Conference on Cyberlaw, Cybercrime & Cybersecurity

‘THE PARTICIPANTS OF THE INTERNATIONAL CONFERENCE ON CYBERLAW, CYBERCRIME AND CYBERSECURITY HEREBY FURTHER CALL UPON UNITED NATIONS AND ITS VARIOUS AGENCIES INCLUDING ITU, UNESCO, WIPO AS WELL AS ALL INTER-GOVERNMENTAL ORGANIZATIONS (IGOs) & NGOs

1. To understand that the issue of jurisdiction needs to be tackled in the context of cybercrimes;

2. To explore the drafting of an international legal instrument on the issue of Cybersecurity;

3. Understand that the emergence of cybercrimes puts people in developing and under-developed countries at serious risk of exploitation;

4. To update the existing treaties on outer space, keeping in mind the latest advancements in cyberspace, both technological and legal changes at the national levels;

5. Ensure that technologies like artificial intelligence do not violate the most cherished human rights;

6. To identify a global definition of cyber-sovereignty to be adopted by nations;

7. To call upon tech companies to work with governments and find solutions to ensure the safety and security of citizens, without eroding user privacy or cyber security;

8. To collaborate with various international, regional and national stakeholders to work together in the development of legal jurisprudence on cyberspace;

9. To strengthen the cooperation on Cybersecurity law, by creating more opportunities for governments, private sector, civil society, the technical community and academia from various regions of the world to engage and develop innovative and effective legal frameworks, to address the truly global challenge of Cybersecurity;

10. To help in deciding as to how Metaverse must be regulated and to educate people about the cyber legal ramifications of highly interactive and inter operable nature of the Metaverse;

11. To encourage the development of effective instruments on cyber-diplomacy, since this diplomacy will be needed due to the lightening fast advancements made in technology;

12. Effectively address the issue of removing the vacuum on cyber security law existing on the international level and provide aid to states not having their own municipal law on the issue of Cybersecurity;

13. To come up with a common understanding at the international level on how principles of cyber sovereignty have to evolve and how conflicts between different cyber-sovereignties of different jurisdictions need to be resolved;

14. To holistically take up comprehensive viewpoints on emerging technological paradigms in cyberspace;

15. To invite the conference's deliberations and expertise in the various UN bodies and processes for the purposes of appropriate dissemination of expertise on various cutting edge issues concerning cyberspace, Cyberlaw, cybercrime and Cybersecurity;

16. To encourage the developments of norms concerning responses to breaches of cybersecurity by nation states and their relevance in the international scenario;

17. To explore identification of common legal principles, which can be made applicable concerning breaches of cybersecurity in outer space and push for their appropriate acceptance and therefore, pre-regulation by various nation-states;

18. To work towards specifically protecting women and children and other vulnerable sections of the human population against constant abuse, misuse and targeting on the internet and in cyberspace;

19. To contribute towards the gradual evolution of cyberlegal jurisprudence at the international level;

20. To encourage countries to come up with stronger national laws on cybercrime so as to deal with the growing menace of cybercrime;

21. To help generate discussions and debate about legal principles impacting cybersecurity which can be adopted at the international level by various countries;

22. To encourage more enhancement of capacity building amongst all nations states specifically on the intersection of Cyberlaw, Cybercrime and Cybersecurity;

23. To encourage nation states to disseminate more information about and encourage the adoption of cyber-resilience as a way of life amongst various nation states and their respective digital stakeholders;

24. To invite the contribution of the conference and its various experts to various initiatives and processes in the intersection of Cyberlaw, Cybercrime and Cybersecurity

25. Suggest ways by which international instruments relating to cyberspace can be made applicable to all countries;

26. To encourage that the emerging trends of cyberspace are not left unregulated and that in the absence of international instruments and municipal laws, there need to exist self-regulatory mechanisms on the national and international level;

27. In the international instruments dealing with cybercrime and cyber security issues, also lay down principles governing how cyber forensics must be conducted and what tools are permissible;

28. To come up with ways to take Public Private Partnerships forward in the cyberspace through ethical and legal means.

THE PARTICIPANTS OF THE INTERNATIONAL CONFERENCE ON CYBERLAW, CYBERCRIME AND CYBERSECURITY HEREBY CALL UPON NATION STATES, EDUCATION & RESEARCH INSTITUTIONS, PROFESSIONAL ASSOCIATIONS, MEDIA INSTITUTIONS, CULTURAL & SOCIAL INSTITUTIONS AND ORGANIZATIONS, NETWORKS, BUSINESS, CORPORATE & INDUSTRY SECTORS AS WELL AS ALL RELEVANT STAKEHOLDERS

1. To come up with dedicated legal frameworks on Cybersecurity as well as to examine and explore the elements of cyber-resilience emerging in the digital ecosystem and the connected legal, technical and other logistical elements that are evolving to be integral parts of the cyber-resilience paradigm;

2. To come up with more innovative projects, initiatives and exercises aimed at identifying some of the emerging cutting edge trends that are emerging in the cyber landscape;

3. To explore how the issue of online gaming is beginning to throw up complicated issues for all stakeholders;

4. To work on commonly accepted principles for regulation of fake news and dissemination of fake information on social media, internet and cyberspace at large;

5. To work in the direction of creating more safe, secure, reliable and resilient cyber ecosystem and to work in the direction of creating cybersecurity as a way of life;

6. To explore how the legal and policy challenges thrown up by metaverse can be appropriately regulated in a minimal way;

7. To explore how cyber-hygiene practices have to be disseminated amongst all stakeholders in the digital ecosystem on a continuing basis in order to contribute into making the cyberspace more safe, robust and reliant;

8. To regulate online abuse, cyber bullying and online defamation, since the internet is the fastest mode of communication and it is important to come up with ways to safeguard a person's reputation from being falsely tarnished;

9. To come up with data ethics for each industry and sector in accordance with the unique needs, working method and business model of each industry and sector;

10. To come up with self-regulatory mechanisms to control technology and to ensure relevant mechanisms are in place to protect data of consumers, customers and all those whose data is stored;

11. To make the armed forces technologically advanced enough to ward off attacks on a nation's sovereignty in the cyberspace;

12. To specially focus on ransomware, which is readily available on the darknet;

13. To enter into cyber diplomatic agreement with foreign actors;

14. To understand that the emergence of metaverse is significant not only for gamers, but also for lawyers since it creates new kinds of legal issues, like Intellectual Property Rights issues, criminal issues and hence, new laws need to be made accordingly;

15. To come up with a definitive regulatory mechanism on the blockchain technology, since it is responsible not only for creating a whole new man-made currency which can be easily converted into fiat currency, but may very well be the future of the internet in the form of Web 3.0;

16. To keep the growing power of social media intermediaries in check and to not make them super powerful as well as to try and put a stop on cyber bullying, with the act negatively discouraging people from freely exercising their freedom of expression;

17. To come up with a definitive law on mobile apps, with handheld devices slowly replacing devices like desktops and other stationary devices;

18. To make a proper law on Telemedicine to cover the legal issues connected therewith and to lay down specific guidelines as to the extent to which Telemedicine can be practiced and a patient be diagnosed without being near the doctor physically;

19. To find solutions to the threats posed to information infrastructure by cybercrimes like phishing, identity theft and fraud including encouraging crystallization of holisitic legal, policy and regulatory responses to tackle the menace of the aforesaid infamous trinity of cybercrimes;

20. To identify the threats to the banking and financial sector and Insurance services due to cyberattacks and measures that can be taken to ensure preparedness;

21. To identify the cyber security aspects of space satellite ecosystem and its profound impact on a myriad of sectors and activities built on the satellite information systems, thus reiterating the interlinkages between cyberspace and outer space;

22. To bring into focus the challenges presented by new technologies such as deepfakes, promote awareness of new technologies and accompanying potential risks connected therewith;

23. To work towards ensuring that the security of upcoming 5G technology is paramount as well as to identify the legal principles and frameworks required to deal with the cyber security and technical challenges thrown up by the advent of 5G;

24. To coordinate, share, monitor, collect, analyse and forecast, national level threats to CII for policy guidance, expertise sharing and situational awareness for early warning or alerts as well as to engage in the risk analysis process, and related mitigation or counteraction strategies;

25. To make sure that an AI system does not hamper fundamental rights, thanks to various strategies including certification, tests, periodic checks, open source code analysis;

26. To ensure support for appropriate privacy and personal data protection and to work towards safeguarding personal data and privacy in the age of the internet, promoting awareness both of technologies and potential risks;

27. To provide a catalogue of security related institutional legal controls to meet current information protection needs and the demands of future protection needs, based on changing threats, requirements and technologies;

28. To identify, though an interdisciplinary approach, the future possibilities, scope and impact of emerging technologies such as IoT, Artificial Intelligence and Machine Learning as well as to identify future emerging technologies (FET) and the legal, policy and regulatory issues related therewith.

WE, ICCC PARTICIPANTS, URGE THAT JOINT EFFORTS NEED TO BE TAKEN BY ALL RELEVANT STAKEHOLDERS TO MAINTAIN THE INTRINSIC CHARACTER OF CYBERSPACE WHICH IS SAFER, MORE RESILIENT, AND REMAINS THE MAJOR DRIVER OF SUSTAINABLE ECONOMIC DEVELOPMENT AND GROWTH FOR YEARS TO COME.

WE REITERATE THAT STEPPING FORWARD IN A NEW ERA OF DIGITAL AND CYBER WORKSPACE, WE ALL NEED TO BE SAFE, SECURE AND DILIGENT, WHILE ENCOURAGING FURTHER ADVANCEMENT IN CYBERSPACE AS WELL AS INFORMATION AND COMMUNICATION TECHNOLOGIES (ICTs).

WE, THE PARTICIPANTS OF THE INTERNATIONAL CONFERENCE ON CYBERLAW, CYBERCRIME AND CYBERSECURITY, APPROVE AND ADOPT THE ABOVE OUTCOME DOCUMENT.