INTERNATIONAL CONFERENCE ON CYBERLAW, CYBERCRIME & CYBERSECURITY

OUTCOME DOCUMENT 2023

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

29th November to 1st December, 2023
New Delhi,India

OUTCOME DOCUMENT

OF THE

INTERNATIONAL CONFERENCE ON CYBERLAW, CYBERCRIME & CYBERSECURITY

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

29th November – 1st December, 2023

(New Delhi, India)

(10TH EDITION)

THEME

"RISE OF ARTIFICIAL INTELLIGENCE, EMERGING TECHNOLOGIES AND THEIR IMPACT"

Prominent Supporters – ICCC 2023

PREAMBLE

UNDERSTANDING that emerging technologies are developing like the evolution of humanity;

REPEATING that in the coming times, these emerging technologies will be a fresh source of worry;

STATING that the policy and related voids created by the emergence of these technologies need to be filled up with expediency;

EMPHASIZING how the cyber-security challenges created by these new emerging technologies pose a risk for individuals, entities, businesses and for all stakeholders;

APPRECIATING how the stakeholders of all types have come together to support the conference;

RECOGNIZING that cyber-security is the need of the hour, not only on the part of the government entities but also on the part of the citizens;

FOCUSING on how the sudden popularity of Generative AI can lead to a plethora of misinformation;

ACCEPTING that the current laws on Artificial Intelligence, in many parts of the world, need to be updated in order to meet the rising challenges;

ACKNOWLEDGING that although the threat to the world as we know is immense, there are efforts being made by both governmental and non-governmental stakeholders to counter such threats;

WITNESSING how deep fake videos are being circulated on the internet as genuine, leading to a severe fake news infodemic;

UNDERLINING how the Intellectual Property Rights of creators are now at risk of being easily plagiarized, thanks to the emergence of Generative Artificial Intelligence;

NOTICING how Generative AI, while being a boon for some people, is equally bane for other people due to the absence of any legal regulation and that Generative AI is the mercenary of the online world as some would benefit from it and others would suffer;

RESTATING the importance of Zero Trust Security, especially in the background of increasing cyber-attacks on entities across the world;

AGREEING that it is in the best interests of both government and non-government stakeholders to deploy zero trust;

APPRECIATING that IT teams in many organizations, entities and other bodies have already rolled out Zero Trust, however, in the absence of specific regulations, many struggle in their journey;

SEEKING solutions for the problems arising in protecting data and ensuring the online privacy of individuals;

SEEKING remedies for crimes committed using Artificial Intelligence;

ATTEMPTING to understand the benefits and harms of adopting the different approaches in combating cybercrimes;

AGREEING that the intersection of Cyberlaw, Cybercrime And Cybersecurity will grow due to the emergence of new and modern technologies and its impact will be felt on the whole world.

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 the legalities of emerging technologies;

2. To investigate the impact of these new technologies on cybercrimes;

3. To see how these technologies affect the basic rights, freedoms and liberties of individuals, entities, bodies, citizens and non-citizens;

4. To look at the geo-political developments evolving due to these technologies;

5. To see that investments made in Artificial Intelligence, after the emergence of popular Generative AI software, does not result in the AI companies becoming un-proportionally powerful.

6. To look for ways to attribute the criminality of the AI crimes to a real person or a body, whether the victim and accused are sitting in the same jurisdiction or not;

7. To discuss, analyse, study and disseminate the recommendations of the International Conference on Cyberlaw, Cybercrime & Cybersecurity 2023 to the relevant stakeholders;

8. To work with all stakeholders via networking, interacting, collaborating and discussing on the various aspects pertaining to emerging technologies and come up with ideas as to how such technologies can be regulated, controlled, their harmful effects minimized to controllable levels;

9. To become a catalyst for the key discussions on the effects on cyberspace of such emerging technologies and try and keep updated with the latest trends, developments and updates in such technologies;

10. To try and come up with a legal definition of the ‘Zero Trust’ concept, which will be applicable on an international level;

11. To contribute towards coming up with an international jurisprudence on crimes that are being committed while using AI;

12. To come up with legal principles to govern the scenarios when the AI itself becomes the perpetrator and how to deal with the legalities of Artificial Intelligence in this direction.

13. To come up with international recommendations on the compliances that need to be followed by corporates, especially in the post-Covid era and more specifically, in light of the emerging technologies coming up;

14. To understand and educate that Darknet is unlike any paradigm seen before and hence, to regulate the activities done on the Darknet, for whatever motive, new approaches will not only have to be adopted but will also have to be incorporated in the cyber-laws, cyber-crime laws and cyber-security laws of each jurisdiction;

15. To make recommendations for strengthening the law-enforcement agencies across the world so that they can effectively counter the threats being raised by criminals and malicious actors using Darknet for their nefarious activities;

16. To convince the government to come up with more laws, notifications, rules and regulations dealing with the electronic health records of individuals, since the electronic health records of individuals have been proved to be both most valuable for and most vulnerable to cyber-criminals;

17. To explore and recommend the various options of enterprises coming up with their own safeguards for preventing cyber-security breaches, including putting in place appropriate policies which lay down the response mechanisms when an enterprise learns that it has become a victim of a cyber-breach;

18. To highlight the gaps often seen in the response mechanism and policies of enterprises, when such enterprises first learn that they have become victims of cyber-security breaches.;

19. To recommend increasing dialogues between CISOs, lawyers, policy experts and other entities which can look at how the emerging technologies are affecting the law and legal scenario everywhere.

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 INTERGOVERNMENTAL ORGANIZATIONS (IGOs) & NGOs

1. To discuss and elucidate clarity about Darknet and to come up with common legal accepted principles concerning the regulation of Darknet;

2. To hold meetings between various nation states as to decide on coordinating the investigations of cyber-crimes, cyber-security breaches and other data breaches done using Darknet;

3. To see how the electronic health data of individuals can be exposed or otherwise negatively impacted by emerging technologies and arrive at commonly accepted principles as to how such data needs to be protected;

4. To form international instruments/understandings on mobile apps in particular and the mobile ecosystem in general, since various malicious activities can be done using such mobile apps;

5. To address the issues raised by the data economy and recognise data economy as a new rising economy, especially in the light of emerging technologies which have made data the new oil as well as to track the developments of Web 3.0 and lay down international standards, recommendations and guidelines on how the online ecosystem should function, in the age of Web 3.0 as a reality;

6. To look at the emergence of cyber-diplomacy and see how treaties or other international instruments can be made using cyber-diplomacy;

7. To encourage nation states that countries regulate the spread of fake news and make sure that there is a strict but non-discriminatory attitude towards those who spread fake news;

8. To come up with effective guidelines, standards and legal protections for the bodies forming the Critical Information Infrastructures, so that such infrastructures are not likely to be vulnerable to cyber-security threats;

9. To encourage the exploration of the evolving ethical principles concerning Artificial Intelligence and see how the said ethical principles could be incorporated in the national legal frameworks on Artificial Intelligence;

10. To analyse the emerging concept of cyber sovereignty and try to explore various legal principles which are informing the growing evolution of jurisprudence concerning cyber sovereignty and how cyber sovereignty could potentially create more challenges for the application of international covenants and instruments of international law, given the changing ground realities of cyberspace.

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 emerging technologies;

2. To examine and explore the essential challenges in the area of emerging technologies paradigm and the connected legal, technical and other logistical elements that are evolving to be integral parts of the cyber-resilience paradigm;

3. To look up ways, in coming up with new legislations, rules, orders, regulations or by investing in the required technologies, for strengthening the Critical Information Infrastructure of countries;

4. To formulate guidelines for using Generative AI tools, in the absence of effective enforcement mechanisms;

5. To come up with laws which lay down minimum requirements for mobile apps to be made available in a particular jurisdiction;

6. To lay down laws, rules and regulations laying down the extent of applicability of cyber sovereignty of governments over activities done in the cyberspace;

7. To formulate laws in the form of legislations, rules, order, regulations etc. which curb the spread of fake news on the online ecosystem, especially when the use of any emerging technology is involved;

8. To enable and regulate the technology of cloud computing and to come up with a specific law which regulates the use of this technology;

9. To encourage the need for coming up with broad international principles on legal recognition and regulation of AI at the international level;

10. To come up with the national laws to deal with various aspects of not just Artificial Intelligence but also Generative Artificial Intelligence and its applications in various fields;

11. To ensure that the misuse of emerging technologies like Artificial Intelligence for criminal purposes needs to be quickly regulated;

12. To recognize that the advent of AI crimes represents new alarm bells for the digital stakeholders and appropriate steps need to be taken to enhance the coverage of existing laws to include within their ambit, Artificial Intelligence crimes and emerging tech crimes;

13. To encourage the recognition that emerging tech crimes like AI crimes need to be specifically brought within the ambit of criminal laws and effective deterrent punishment needs to be provided, so as to give a message in the early days of adoption of emerging technologies that misuse of emerging technologies like AI for criminal activities, terror purposes or money laundering could invite serious consequences for the requisite stakeholders;

14. To foster more discussion and debate at the international level on the various legal nuances and legalities thrown up by emerging technologies like Artificial Intelligence. The entire issue of hallucination of data in Artificial Intelligence needs to be collectively addressed by nation state actors as also by the industry at large;

15. To recognize the need for further common understanding on broad ethical principles that need to be agreed upon in the context of their applicability as far as AI and Generative AI is concerned;

16. To emphasize the need for more clarity and transparency in terms of evolving international practices that could cover the advent and growth of responsible AI;

17. To underline and reiterate the importance of audits for preventing or minimizing bias or discrimination in AI algorithms and to encourage all stakeholders to go for voluntary auditing of their AI offerings and algorithms so as to minimize the problem of bias and discrimination of the said AI programs and algorithms;

18. To develop common normative norms for determining the legal liability as a result of harm or injury caused by reliance on output of AI to various stakeholders;

19. To understand and appreciate the misuse of emerging technologies like Artificial Intelligence for breach of cyber security as a major challenge that is emerging with the passage of time and to encourage the taking of appropriate steps by international and national stakeholders so as to minimize the impact of cyber security breaches caused by or powered by Artificial Intelligence;

20. To recognize the growing prevalence of cybercrime-as-a-service powered by Artificial Intelligence and to call upon the nation states to come up with effective mechanisms to deal with the regulation of cybercrime-as-a-service powered by Artificial Intelligence;

21. To appreciate that the emergence and advent of emerging technologies like Metaverse, Quantum Computing, IoT and Blockchain bring forward new vistas of opportunities and challenges from holistic perspective for all stakeholders;

22. To acknowledge that change is the only constant and that emerging technologies today are once again underlining the fact that digital ecosystem stakeholders have no choices but to be constantly ready for adopting to constant new changes in the technological paradigm;

23. To recognize that there is need for creating and enhancing more capacity building as far as use and application of newly emerging technologies in different facets and vistas of digital activities and data economy ecosystem;

24. To examine the societal impact of emerging technology and to take appropriate steps to ensure that the negative aspects of emerging technologies do not prejudicially impact societies, societal stakeholders as well as also societal norms;

25. To recognize that the quantum increase in efficiency of emerging technologies represents an elephant in the room for the sovereignty, security, integrity of countries and also to their cyber sovereign interests. Hence, nation states need to be mindful of the impact of these emerging technologies on national interests and need to take appropriate steps to ensure that the national interests do not get prejudicially impacted by the advent and misuse of such emerging technologies;

26. To acknowledge the Emerging Cyber World Order that is engulfing the world post Covid-19 and recognizes the advent and adoption of newly emerging technologies as an intrinsic component and part of the New Cyber World Order;

27. To reiterate that appropriate holistic strategies need to be adopted by countries so as to come up with dedicated new legal frameworks concerning protection and preservation of cyber security and to increasingly recognize the connection between cyber security and national security;

28. To work towards the evolution of appropriate normative norms at the international levels so as to promote the cause of protection and preservation of cyber security, given the use of AIs in warzones, and potential war crimes committed by AIs;

29. To work towards urgent immediate action by nation states to put up a determined fight against cybercrimes, given that cybercrime is leading to countries and their economies bleeding with growing global costs;

30. To encourage countries to have dedicated cybercrime laws so that they can come up with appropriate effective deterrent mechanisms to fight the menace of growing cybercrimes;

31. To sensitize countries to specifically come up with effective and efficient electronic evidence strategies and legal frameworks which can help aid the increasing of cybercrime conviction ratio of different nations;

32. To formulate laws, in the light of the vulnerable position of women and children in the online world, which protect them from online harassment and victimization, especially when such women and children belong to marginalized groups;

33. To understand that groups that have been discriminated against in the physical world, have also been discriminated against in the online world and thus, extend the human rights jurisprudence to them in the online world also by formulating certain laws, whether such laws are primary or secondary legislation;

34. To come up with laws on blockchain and to create a cryptocurrency network across the world, which is in sync with the global banking network;

35. To recognize that Cyberlaw frameworks of different countries need to be updated so as to make them more topical and relevant given the constantly changing technological ground realities of cyber ecosystem;

36. To encourage the need for having in place common accepted principles of cyber legal jurisprudence at the international level, given the absence of a global cyber legal regime in place;

37. To work on updating legal frameworks so as to deal with evolving legal jurisprudence concerning attribution of acts done using the TOR network and Darknet;

38. To recognize the need for countries to have in place strong legal frameworks for regulating emerging technologies like deepfakes, to prevent their misuse for various criminal and other vested interests;

39. To target the fake news and false information that is continuously polluting the content in the cyber ecosystem;

40. To recognize the need for countries to have in place strong legal frameworks to penalize ransomware attacks and to create appropriate capacity building about the nature, manner, kind and impact of ransomware attacks and how to enable digital stakeholders for coming up with appropriate mitigation strategies to prevent the prejudicial impact of ransomware attacks on computer systems, networks and data;

41. To encourage countries to adopt legal frameworks and industry best practices pertaining to zero trust in order to safeguard their computer resources;

42. To sensitize countries for the need to come up with dedicated legal frameworks to protect their Critical Information Infrastructure from potential attacks by state and non-state actors;

43. To explore how the misuse of crypto-assets and crypto-currencies could be appropriately regulated, specifically in the context of the use in money laundering activities;

44. To focus also on how Edge Security can be given far more primacy in terms of the national instruments and legal approaches so that the national legal frameworks give appropriate importance and significance to securing the devices connected to the edge of the network;

45. To ensure that effective legal frameworks and appropriate regulatory mechanisms need to be put in place so as to fight the menace of cyber security breaches;

46. To re-emphasize the need for countries to get together to come up with proactive cooperation mechanism to share information and work jointly to fight cyber security breaches, given the transnational nature of cyber security breaches;

47. To recognize that given the fact that more and more cyber criminals are now increasingly turning onto the darknet and using methodologies to remove their footprints, it has become even more relevant for countries to cooperate with each other on issues pertaining to attribution of criminal activities of concerned cyber actors;

48. To work towards evolution of appropriate international principles for attributing particular cyber activities to particular cyber actors;

49. To recognize that post Covid-19, financial cybercrimes have been massively increasing. With phishing, identity theft, online financial frauds and ransomware on the rise, there is a need for countries to come up with effective frameworks to provide adequate protection to victims of online financial frauds. Through their national legislative processes, countries need to specifically work together on protecting their consumers in cyberspace;

50. To ensure that adequate attention needs to be given for protecting the privacy of individuals in the AI ecosystem where Machine Learning and AI put together, can present actual, concrete and practical challenges to both personal and data privacy;

51. To acknowledge that the problem of deep fake technologies has assumed alarming proportions and it is time for stakeholders to create more capacity building and

awareness about deep fake technologies and its potential misuse against netizens and users;

52. To work together to come up with legal principles to ensure that misuse of crypto-assets for criminal purposes as also for terror purposes is potentially minimised and the said misuse appropriately be made punishable under applicable penal laws;

53. To impress upon Nation states to come up with simpler principles of electronic evidence, given the increasing reliance on electronic evidence and provide more effective approach for producing and proving electronic evidence as admissible electronic evidence in courts of law;

54. The International Conference on Cyberlaw, Cybercrime & Cybersecurity takes note of the advent and emergence of AI crimes like AI kidnapping, AI defamation, AI online financial frauds and AI phishing and encourages nation states to come up with effective legal frameworks to fight the menace of AI frauds.

55. That for the Government of India, the International Conference On Cyberlaw, Cybercrime And Cybersecurity makes the following recommendations: -

    a) To give a clear message to companies and their boards that compliance with applicable laws will have to be the guiding factors for companies and their boards in order to prevent the exposure to potential legal liability, both civil and criminal;

    b) To come up with appropriate national legal frameworks so as to regulate technologies like Artificial Intelligence in every sphere of human activity and endeavour either through mother umbrella legislation on AI or through vertical specific legislations and legal frameworks addressing the specific concerns of specific verticals;

    c) There is a need to amend the Indian cyberlaw to be topical and relevant in today's times;

    d) There is a need for ensuring more adequate coverage of growing kinds of emerging tech crimes under the Indian cyberlaw framework;

    e) India requires a dedicated law on cyber security, which can help protect and preserve the sovereign interests of India in cyberspace, as also to protect its sovereignty, integrity and security;

    f) India needs to adopt new legal frameworks to promote the cause of cyber resilience and cyber insurance.

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 CYBERSPACE, 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.