Cyberlaw University

Phones: +91 11 46584423
Email: info@cyberlawuniversity.com
cyberlawuniversity@gmail.com
Office: C2/60,Janak Puri
New Delhi-110058

24th March, 2022

Ref: AHC/1/2022

To

The Secretariat of Ad-hoc Committee
CybercrimeAHC@un.org

SUBJECT: **WRITTEN SUBMISSIONS ON BEHALF OF CYBERLAW UNIVERSITY FOR THE FIRST INTER-SESSION CONSULTATION OF AD-HOC COMMITTEE**

Dear Sir,

I on behalf of Cyberlaw University would like to submit as under:-

1. One of the most important thrust areas that the proposed convention must deal with has to be cybersecurity. Today, cyber laws, cybercrime and cybersecurity are three sisters who are all intrinsically connected with each other. Today, cybersecurity breaches have become the foundational fountain for the further growth and proliferation of the misuse of ICT networks for criminal purposes. This is having a serious impact because the breach of cybersecurity could have a direct impact upon the enjoyment of national sovereignty and also the entire concept of Cyber Sovereignty. We must realise that the absence of a global international standard on cyber security has also contributed to the current situation.

2. Meanwhile, in 2015, at the WSIS forum organised by the International Telecommunications Union, along with other UN agencies, I had mooted the idea that the world now needs to come up with an International Convention On Cyber Law and Cybersecurity. The idea was a bit ahead of its times, but now, with this ad hoc committee working on this proposed convention, I believe that the elements of the convention need to be holistically defined and detailed so as to not just focus on a narrow vision of the misuse of ICT networks for criminal purposes but also for the purposes of encompassing all elements of breaches of cybersecurity for criminal purposes by ICT networks having an intrinsic Impact upon the digital economy and the need for covering the same within the ambit of the current proposed convention.

3. At the International Commission on Cybersecurity Law, we are looking at how legal principles need to evolve so as to cover the misuse or abuse of cybersecurity, for the purposes of committing various cyber criminal activities. The Perusal of cyber security laws in different parts of the world are increasingly pointing out to some interesting legal trends. I believe that the said legal trends pertaining to evolution of cybersecurity breaches in the digital world today would be an important thrust area for the consideration of this Hon'ble committee and for potential inclusion in the ambit, scope and ultimate elaboration of the provisions of the Convention.

4. We need to realise that we are working in a data economy and in this data economy, preventing the misuse of ICT networks for criminal purposes becomes a topmost priority. Hence, all issues pertaining to the misuse of different aspects of the data economy for criminal purposes are elements that need to be intrinsically made an integral part of the proposed convention.

5. With the convention coming in today's time and age, it becomes essential for the convention to address issues impacting the darknet. Darknet has become the de facto home of the dark net economy where cybercrime is the basic colour that's been colouring the entire landscape. Most of the international conventions have by and large, hesitated from

addressing the issues pertaining to darknet due to the intrinsic architecture of the darknet, but I believe much more needs to be done in this regard. Somewhere down the line, the beginning has to be made and this committee, through this proposed convention, could really make a big thing in terms of trying to address one of the key problems in the global cybercrime ecosystem, which is the darknet.

6. Further, now with increasing use of artificial intelligence, both for the purposes of committing cyber crimes and also for the purposes of fighting cybercrime, it becomes imperative that the proposed convention must give adequate coverage to the exact ambit and scope of emerging technologies like artificial intelligence, specifically in the light of the use of such technologies for the purposes of criminal elements, activities and designs. At Artificial Intelligence Law Hub, we are researching and working on global legal principles for regulation of artificial intelligence. Hence, any activity or initiative aimed at regulating the misuse of AI for cybercrime purposes must necessarily keep in mind the evolving cyber legal principles, which impact the regulation of Artificial Intelligence and its appropriate legal recognition by legal frameworks across the world.

7. Another important thrust area that needs to be specifically focused on, in the context of the misuse of ICT for cybercrime or for criminal purposes, has got to deal with the entire issue of block chain. Block chain has become the foundation for newly emerging kinds of crypto assets and crypto currencies. However, these cryptoassets and cryptocurrencies have already begun to start having a very crucial impact upon the further growth of criminal activities using ICT networks. Therefore, the misuse of crypto assets and crypto currencies for cybercrime purposes is one particular area that needs to be specifically focused by the authors of the proposed convention. This becomes important as different countries are slowly waking up to the need for controlling the misuse of the Blockchain and crypto ecosystem for cybercrime purposes. Recently, the President of the United Stated of America issued an executive order, asking for a more distinctive clarity on block chain and one of the elements is mitigating the illicit finance and national security risks posed by the misuse of digital assets. At Blockchain Law Epicentre, which I'm currently heading as the

Chief Executive, we are aiming to explore the coming of legal foundation, principles and frameworks which can be used for the purposes of preventing the misuse of block chain for cybercrime purposes.

8. A thrust area that the committee must also keep in mind while drafting the proposed convention, is that the convention should also be specifically focusing on emerging technologies like Internet of Things. The Internet of Things today has become a very fertile ground for the propagation of new kinds of cybercriminal activities. The absence of global cybersecurity standards on Internet of things means that it is a virtual melting pot for not just breach of cyber security of IoT systems and networks, but also misuse of IoT devices for the purposes of hoaxing on or committing criminal activities. Hence, the possible misuse of IoT for criminal purposes is one particular area that the convention must particularly be focusing on. We need to be mindful of the fact that this committee is working on a proposed convention and would like to give its total support by 2024. By that time, most of these newly emerging technologies would have become well entrenched and therefore, it will be a crucial element that these aspects of the criminal use of emerging technologies be adequately addressed by the authors of the proposed convention.

9. We also need to understand that the newly emerging technologies like quantum computing are going to fundamentally change the existing perceptions about algorithms and security passwords are soon going to become history, with quantum computing breaking passwords within a couple of minutes or hours. It becomes important to understand that quantum computing is also likely to become a very significant tool in the hands of cyber criminals for the purposes of perpetuating their cybercrime activities. Hence, the crimes relating to quantum computing should be on the distinctive thrust area initiative, especially incorporated as an integral component of the proposed convention.

10. Yet another area which the convention must specifically focus on deals with the newly emerging paradigm of metaverse. Metaverse is the new version of the Internet, the new avatar of the present day Internet and metaverse is going to see massive increase in

spending of time by Internet nerds and netizens. Metaverse is already beginning to see massive amount of misuse of ICT networks for criminal purposes. Metaverse crimes have already begun to start emerging. There is tremendous increase in metaverse crimes which come under the categories of or include metaverse bullying, metaverse harassment, metaverse rape and other metaverse crimes. Hence, any kind of convention that the committee is proposing has to be more holistic, futuristic than the convention currently in force and must also keep in mind the adequate elements pertaining to the metaverse. At Metaverse Law Nucleus, we are already examining the legal frameworks on how Metaverse activities can be legally regulated and how Metaverse crimes can also be appropriately well addressed by legal frameworks. However, this would be an important issue that will have to be taken into consideration by the authors of the proposed convention as we go forward.

11. The world today is beginning a new revolution. I call it "The Great Global Vomiting Revolution". This is the revolution where everybody in the world seems to be vomiting data about their personal, professional, social lives without even thinking anything about the legal ramifications from the same. On top of that, we are all leaving behind digital dust. These are electronic footprints that we are leaving behind without appropriate considerations. It's these very footprints and this digital dust that specifically being focused and extensively exploited by cyber criminals for the purposes of targeting not just individuals, networks, but also ultimately even governments and the sovereign institutions. Hence the importance of digital dust and electronic footprints in the context of the misuse of ICT networks for criminal purposes is yet another thrust area that the proposed convention must specifically be dealing with.

12. Important issues that the proposed convention must also deal with relate to the elements concerning the evidentiary aspects of ICT hard drive activities, having criminal intentions or designs. However, one of the biggest challenges that the world is currently facing is the inability to get appropriate convictions in cybercrime matters and primarily speaking, one of the key reasons in this regard is the inability of the relevant law-enforcement agencies to

get the relevant incriminating electronic evidence to link the particular cyber-criminal activity to the particular cyber actor. Different countries are already having in place different mechanisms relating to electronic evidence, rendering admissions and proving their genuineness. However, this committee while coming up with the proposed convention must also give appropriate thrust areas or the key elements of electronic evidence and must also consider various issues impacting cybercrime and crimes using ICT networks.

13. The entire issue of attribution of a particular cybercriminal activity to a particular cyber actor is a very contentious issue and is something that the convention must be taking into account. This is so because this is one area where not much work has been done. The absence of a global cybercrime law has further complicated the entire scenario. As such, across the world, different countries are adopting their own distinctive approaches on how to deal with attribution of cybercriminal activities. Any convention on the use of ICT for criminal purposes will be incomplete without adequately and comprehensively discussing all the contentious issues pertaining to attribution of criminal activities to particular cyber actors in their entirety.

14. Yet another key element for the proposed convention will have to be the important issue of Internet jurisdiction. Internet has made geography history, or irrelevant, in other words. However, the advent of this boundary-less medium called cyberspace has encouraged countries to come up with their own respective national cyber laws for the purposes of regulating activities within their territorial boundaries. However, it's still possible for a person sitting in one part of the world to use the ICT networks for committing cybercriminal activities targeted on computer systems and servers located in another part of the world. That means determining Internet jurisdiction has become a huge challenge. The absence of a global standard on Internet jurisdiction has further complicated the entire scenario. Hence, one of the key elements that the proposed convention has to specifically deal with is the concept of Internet Jurisdiction. The Convention must concentrate on the elaborate aspects of Internet jurisdiction and must provide aworking practical guidance to

nation-states on how the entire contentious issue pertaining to Internet jurisdiction needs to be specifically addressed.

15. Since the convention is proposed to be dealing with the criminal aspects of the use of ICT networks, it will be very essential that the committee recognises the importance of cyber legal frameworks at national levels. In this regard, globally, there is an absence of international cyber law in place. This policy vacuum on cyber law has prompted different countries to start coming up with their own distinctive national cyber laws under the ageis of and under the inspiration of the United Nations' UNCITRAL model on electronic commerce and the UNCITRAL model of electronic signatures. A number of countries have customised their national/domestic cyber laws in such a manner that they have elements pertaining to cybercrime as an integral component of their own respective national legislations. Hence, it becomes an absolute essential need that the convention must refer to the growing importance of cyber law at an international level and also must subsequently deal with the significance of national cyber legal frameworks while dealing with entire issue of tackling and regulating the misuse of ICT networks for cybercrime purposes or for criminal purposes.

16. Globally speaking, different countries have different penal laws in their own respective jurisdictions. These penal laws are diverse, distinctive and often do not have any universal colour. In a scenario like this, the convention must also appreciate the role of national cyber crime laws which are contributing in the fight against the misuse of ICT for criminal purposes.

17. Any convention on the misuse of ICT networks for criminal purposes is going to be incomplete without adequate focus on capacity building. We have seen globally that these capacities need to be constantly enhanced. Law enforcement agencies need to be constantly trained, as also the judicial and the digital stakeholders need to be constantly sensitized about the newly emerging categories of cyber crimes and criminal activities. In this regard, it becomes a crucial necessity that the convention must recognise the role of

capacity building in the context of cybercrime so as to enhance the empowerment of the digital data economy stakeholders at large. At Cyber Law University, which is online education platform & online university dedicated to cyber laws, cybercrime and cybersecurity, we have been conducting various courses. These courses over the last 3 1/2 years have already been done by more than 27,500 students from 174 countries speaking 53 national languages and these figures constantly show that there is a need for massive capacity building.

18. Hence, it is humbly submitted that the proposed convention must specifically have an element on enhancing capacity building of the relevant stakeholders, impacting the regulation of a criminal activities using ICT networks. Further, there is a need for encouraging public-private partnership in enhancing capacity building in the context of fighting cybercrime and misuse of ICT networks for criminal purposes. This public-private partnership becomes a crucial necessity since the efforts of the nation states have to be supplemented by the private sector's academia and other stakeholders so as to be cumulatively prepared for a more holistic brand of network citizens and netizens. The world is changing. Covid 19 has been a great wake up call.

19. In my book, New Cyber World Order, post Covid 19, I have argued that by the time the nations are victorious against the current and subsequent wave of Covid-19 infections, the world will enter into a new cyber age where a new cyber world order would be awaiting us. One of the key elements of the new cyber world order will be that cybercrime will be an integral part of our daily lives and will be our daily companion. Further, increasing cybersecurity breaches will be the norm and the new normal of the day. In a scenario like this, this convention needs to be mindful of this newly emerging cyber age and new cyber world order that's coming and hence, must focus on encouraging nation-states and other relevant stakeholders in proactively dealing with issues pertaining to regulation of cybercrime and also for preventing cybersecurity breaches.

20. These are some of the key elements that I, as an expert in the area of cyber law, cybercrime as also cybersecurity Law and also in my capacity as Chairman of the International Commission on Cybersecurity believe should be incorporated in the proposed convention. These are the same issues which Cyberlaw University, as an academic institution, endorses and we would humbly submit that the said issues be taken up for consideration by the said ad-hoc committee.

It is our humble request that:

1) Cyberlaw University be made an academic rapporteur of this committee and to be allowed to be associated with the committee to help it collate the various thought processes, inputs and perspectives from various stakeholders. At Cyberlaw University, we will further be happy to provide our expertise to this distinguished group;

2) Cyberlaw University would be happy to help this Committee by becoming a catalyst which collates the various perspectives, thought processes, opinions, visions and also concerns of various digital stakeholders and presenting them before this committee, for the purposes of this Committee's consultation and consideration. For this, Cyberlaw University would be happy to be associated with this Hon'ble committee as a niche specialised academic stakeholder, aiming to bring the emerging cutting-edge issues impacting the subject area;

3) Cyberlaw University would also be happy in providing this Committee with a coverage of the aspects in the proposed convention and connected developments for the consideration of ts various members and for them to make their own appropriate viewpoints on the same. Cyberlaw University would be honoured and delighted to assist the ad hoc committee as an academic rapporteur;

4) I, Dr. Pavan Duggal, would be honoured and privileged to contribute my expertise on cyber laws, cybercrime and cybersecurity as also emerging technologies and the relevant connected legal issues and frameworks to the deliberations of the committee.

Thanking you

Yours Faithfully

Dr. Pavan Duggal
Advocate, Supreme Court of India
Founder-cum-Chancellor, Cyberlaw University