Indonesia's Submission
Views on Scopes, Objectives and Structures (Elements) to the Ad-Hoc Committee to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes

I. General Background and Objectives

1. As one of the world's largest internet users, Indonesia recognizes the importance of information and communication technology (ICT) for society. However, advances in information and communication technology have been exploited for irresponsible behaviour, most notably cybercrime and cyberterrorism, undermining the use of ICT for political, economic, and social development.

2. Cybercrime, like other transnational crimes, has affected international community due to the unique and borderless nature of technology and cyberspace. Thus, international cooperation is critical. Indonesia commends the adoption of Resolution 74/247, which establishes an Ad-Hoc Committee to elaborate a comprehensive international Convention on countering the use of information and communications technologies for criminal purposes.

3. Indonesia believes it is very timely and critical to discuss the specific cybercrime convention within the framework of the Ad-Hoc committee, and hopes that states will seize the momentum to discuss and negotiate an international instrument capable of responding to cybercrime challenges, in an inclusive and transparent manner.

4. Over the last decade, significant progress has been made in the discussion and development of international instruments aimed at determining the most effective methods of cybercrime prevention. As a result, when considering a future cybercrime instrument, states should consider all existing platforms and frameworks, including the work of the intergovernmental expert group (IEG) on cybercrime and UNTOC.

5. The discussion on the cybercrime convention shall primarily aim at enhancing and promoting international cooperation in support of national, regional, and international efforts to combat the use of information and communications technologies for criminal purposes, including by providing technical assistance to improve member states' national legislation and frameworks and build the capacity of national authorities to deal with such crimes.

6. Furthermore, the convention shall take appropriate and effective measures between and among states, as well as, as applicable, in collaboration with relevant international and regional organizations.

II. Principles

7. As with many international conventions, our consideration should reflect member states' obligations in accordance with the principles of sovereign equality and territorial integrity of states, as well as non-interference in the domestic affairs of other states. Furthermore,

states should respect the sovereign rights of other states when developing policies and legislation to fight cybercrime in accordance with their national conditions and needs.

8. The future instrument must recognize the impact on security, social, economic and humanitarian consequences of the use of information and communication technology for criminal purposes. At the same time, the convention will ensure that measures to combat cybercrime will focus on the criminal behaviour and do not jeopardize the development of ICTs, including research, development, and technology transfer.

9. It is in the interest of all and vital to the common good to promote the use of ICTs for peaceful purposes. Respect for sovereignty, human rights, fundamental freedoms, as well as sustainable and digital development, remain central to these efforts.

10. Indonesia also sees the merit of ensuring that criminal procedures are established, implemented, and applied in accordance with each nation's domestic law, while also acknowledging the need to address challenges of criminal procedures differences in each state, as well as each state's obligations under relevant international instruments, such as UNTOC, international human rights, intellectual property rights, and bilateral extradition and/or mutual legal assistance treaties.

11. Furthermore, member states must stress the need of maintaining an open and transparent multi-stakeholder process that allows all Member States to negotiate in good faith toward informed, consensus-based, realistic solutions.

III. Scopes

12. The scope of the convention must be able to address current and future challenges of misuse of ICTs for criminal purposes, protect ICT users, and mitigate and prevent harm to people, data, systems, services, and infrastructures.

13. The convention should also be able to ensure that members be able to adopt legislative and other measures as may be necessary to establish as criminal offences from undertaking activities prohibited by the convention, in particular computer crimes, computer-related crimes, and for further illegal ends.

14. Indonesia believes that the future convention should cover a whole range of core cybercrime offences. These are including **but not limited to**:
    a. illegal access to or hacking into computer systems;
    b. illegal interception of computer data and system;
    c. fraud;
    d. misuse of computer data and system for criminal purposes;
    e. copyright and related rights infringements;
    f. manipulation of computer data and system;
    g. distribution and transmission of illegal contents and materials, for example, pornography, child pornography, disinformation, conspiracy, hoax, material that contains racial, nationality, religion or political based hostility;

15. Member States shall consider adopting the measures required to carry out the criminal proceedings outlined in the convention, including, **but not limited to**:

a. data and system preservation, preservation of traffic data stored by a single or multiple service providers, and note that the timeframe for the preservation of data and the classification of stored data in its territory are regulated under national and domestic law.
b. submission or transfer of stored computer data by individuals or legal entities, and to find adequate measures to compel the online system service providers to submit or transfer stored computer data, including data related to the type of services.
c. search and seizure of data and computer systems; the creation and preservation of a copy of computer data; and the modification and transfer of data storage.
d. collection and recording real-time traffic data, as well as to obtain the traffic data from the online service/system providers.

16. Taking this into account, Member States should ensure that the cybercrime investigation process is carried out in accordance with the principles of privacy protection, confidentiality, public service sustainability, maintaining the continuity of public services, and upholding the public interest, as well as data integration.

IV.Cooperation

17. Cybercrime and crimes facilitated by the use of ICTs should be investigated effectively at the national level and transnationally. Thus, the instrument should serve as an effective mechanism for international cooperation in combating the use of ICTs for criminal purposes. Such collaboration should be implemented on the basis of mutual benefit and reciprocity in accordance with national legislation, taking into account existing instruments and ongoing mechanisms/frameworks.

18. Given the importance of multi-stakeholder approaches to cybercrime prevention, detection, and eradication, the discussion should also focus on fostering strong with entities and cybercrime cooperation, including cooperation between law enforcement authorities and ICT service providers. Collaboration with private enterprise, backed up by public-private partnerships when feasible, is crucial in this context for improving knowledge and increasing the effectiveness of cybercrime responses. Member states should also invest in raising awareness of cybercrime in the public and private sectors.

19. Our deliberation should also highlight measures to allow authorities to conduct investigations where data gathering, and confiscation occurred through mutual legal assistance mechanisms, and member states may consider using their existing legal frameworks in this regard.

20. In regards to mutual legal assistance, our deliberation shall be afforded to the fullest extent possible under relevant laws, treaties, agreements, with respect to investigations, prosecutions and judicial proceedings. Among other things, Member States are encouraged to discuss arrangements to expedite collection of electronic evidence or sharing information mechanisms between relevant authorities.

21. The provisions of international cooperation in this convention must provide an essential legal framework in addressing procedural challenges, gap and insufficient mechanisms in international cooperation, especially in investigations, information sharing, data/electronic evidence collection, and prosecution, as well as facilitating extradition

among states. Member states are also encouraged to appoint contact point(s)/authority to expedite the implementation of international cooperation provision under the convention.

22. Furthermore, Member States may consider strengthening national capacity to detect, investigate, and respond to the use of ICTs for criminal purposes, through capacity building and technical assistance efforts that helps and contribute to increasing resilience of member states. These capacity building measures shall build based on mutual trust and demand driven that corresponds to nationally identified needs and full recognition of national ownership

23. As collaboration in preventing and eradicating cybercrime remains a priority in our discussions, the future instrument should at the very least include a list of activities to improve cooperation through the following measures:
    a. Sharing of information on cybercrime threats;
    b. Fostering of enhanced cooperation and coordination among law enforcement agencies, prosecutors and judicial authorities;
    c. Sharing of best practices and experiences related to the cross-border investigation of cybercrime;
    d. Engagement with service providers through public-private partnerships in order to establish modalities of cooperation in law enforcement, cybercrime investigations and evidence collection;
    e. Development of guidelines for service providers to assist law enforcement agencies in cybercrime investigations, including with regard to the format and duration of preservation of digital evidence and information;
    f. Development of human skills and human resources in policies enabling member states to increase resilience towards digital technologies.
    g. Strengthening of the technical and legal capacities of law enforcement agencies, judges and prosecutors through capacity-building and skill development programmes.

24. Through this mechanism, member states should also continue to improve the effectiveness of domestic inter-agency coordination and synergies, including information sharing, and engagement with regional organizations, the private sector, CERTs/CSIRTs, civil society organizations, and other stakeholders to facilitate efficient international cooperation.

25. The discussion should also include a mechanism for reviewing the application or implementation of all commitments and obligations under the future instrument.

-o0o-