

Madam Chair

Excellencies,

Distinguished Delegates

1. To begin, I would like to use the opportunity to thank you, Madam Chair, for your industrious effort in convening this second session of the Ad hoc Working group to continue the elaboration of a global convention on countering the use of information technologies for criminal purposes.
2. In today's era of rapid globalisation, ICT and digitalisation play a key role and have significantly helped in job creation, socio-economic development, education and what have you.
However, the challenge is that the more digitalised our lives become, the more prone we are to cyber-attacks and become potential victims of cybercrime.
3. Accordingly, Madam Chair Ghana welcomes the consideration of a global convention to counter the use of ICTs for criminal purposes. An elaborate convention would complement existing national, regional and international instruments to address the cybersecurity challenges of our time and enhance the safety and security of the cyberspace. Ghana acknowledges instruments such as the UN Convention against Corruption (UNCAC), the UN Convention against Transnational Organised Crime (UNTOC), the African Union Convention on Cybersecurity and Personal Data Protection (the Malabo Convention) and the Convention on Cybercrime (Budapest Convention).
4. As part of Ghana's contribution to shaping the discussion in the development of the Convention, particularly the general provisions of the Convention, provisions on criminalisation and procedural measures and law enforcement, we have submitted the proposed text for consideration on the 12th of April 2022. Madam Chair, with your kind permission, we narrate a summary of our proposed text.

Madam Chair,

5. Ghana is of the view that the general provisions of the Convention should define some key terms. In defining, technology-neutral words should be employed in order to stand the test of time. Additionally, the general provisions should define the scope of the Convention to include application to the prevention, investigation, and prosecution of the use of ICTs for criminal purposes; application to the collection of evidence in electronic form of a criminal offence and assurance of the existence of provisions on freezing, seizure, confiscation and return of proceeds of offences. We are also of the view that under the general provision, member states must guarantee the respect of fundamental human rights and freedoms, privacy, and sovereignty of

states in line with obligations under existing international, regional, and national instruments.

6. Madam Chair, distinguished Delegates, Ghana proposes that the provisions on **Criminalisation** should oblige member states to criminalise in their domestic legislation conduct against the confidentiality, integrity and availability of computer systems and data (cyber-dependent crimes). We advocate explicit provisions regarding Unauthorised access to a computer system, Unauthorised access to a critical information infrastructure, Unauthorised interception, Data Interference, System interference, and Misuse of Device.
7. Further, the Convention should criminalise cyber-enabled crimes where the use of a computer increases the scale, scope, and speed of the offence. Accordingly, Ghana proposes the criminalisation of the conduct of Computer-related forgery, Computer-related fraud, Offences related to online child sexual exploitation and abuse, Cyber-grooming of a child, cyberstalking of a child, sexual extortion, non-consensual sharing of an intimate image, threat to distribute prohibited intimate image or visual recording, Offences related to infringements of copyright and related rights, inchoate offences, and corporate liability.
8. As defined in Article 2 of our proposed text for the Convention about unauthorised access to a Critical Information Infrastructure (CII), a CII means a computer or computer system identified by a member state in its domestic legislation as essential for national security or the economic and social well-being of citizens.
9. Drawing inspiration from Article 25(4) of the African Union Convention and Section 35 of Ghana's Cybersecurity Act, 2020 (Act 1038), Ghana has designated 13 sectors of her economy such as Health, Education, and water to ensure the protection of CII. There are directives for the owners of CII to comply with to enhance the protection and cyber resilience of CII. Last year, the world recorded the reported cyber-intrusion aimed at actively sabotaging the systems that controlled a city's critical infrastructure water system, which could have potentially led to the loss of thousands of lives. The incident tells how imperative it is for state parties to put stringent measures in place to protect our CII and the citizenry at large, including criminalising unauthorised access to CII. The successful prosecution of offences against CII with an accompanying severe sanction will serve as a deterrence to perpetrators.
10. The objective of criminalising the conduct of Unauthorized Access to a CII as opposed to Unauthorised access to a computer system is to help cater for the aggravated conditions presented by the intersection of Unauthorised access to a computer system and the fact the computer system is a Critical Information Infrastructure. This is beside the effects of the act of Unauthorised access to computer systems that may serve a single individual or fewer number of persons.

11. Further on the subject of criminalisation of offences against children online, Ghana is of the view that online child sexual exploitation and abuse, such as the publishing, distribution, and particularly live streaming of child sexual abuse, must be criminalised. Online live streaming of child sexual abuse is one of the newest forms of child sexual exploitation created as a result of technological developments. It is argued that current existing legislation is not sufficient to tackle the phenomenon of live streaming of child abuse. Additional legislation is required, especially in national laws, which would specifically address the offence of live streaming of child abuse. Madam Chair, our future convention should make provision for this.

12. The criminalisation of online child sexual exploitation and abuse aims to ensure the protection of the rights and integrity of children online from the activities of cybercriminals. Also, recall that under Article 34 of the United Nations Convention on the Rights of the child, States Parties are required to protect the child from all forms of sexual exploitation and sexual abuse, taking all appropriate national, bilateral and multilateral measures.

Madam Chair

13. We are of the firm belief that in consideration of the elaboration of a global convention to counter the use of ICTs for criminal purposes, sexual offences such as sexual extortion, non-consensual sharing of an intimate image amongst others must be criminalised under the convention.

14. Such online sexual offences disproportionately affect women and girls. They are increasing at an alarming rate as the internet has increased the scale, scope and speed of the offence. Meanwhile, laws to criminalise the conduct are developing at a snail's pace. In the absence of specific laws, prosecutors rely on traditional laws to prosecute specific issues of violence against women online, which may end up in some form of injustice; because traditional laws are unable to address intersectional matters associated with online sexual offences. Therefore, it is imperative that the future convention obliges signatory member states to adopt specific provisions to address online sexual offences. Ghana has proposed text in that regard.

15. Madam Chair, Ghana underscores the need for the future Convention to strengthen the investigatory, prosecutorial, and judicial powers and procedures of Criminal Justice Authorities in combatting cybercrime at the national and international levels. Appropriately, we propose that the Convention should explicitly contain provisions on
 - a. Expedited preservation of stored computer data
 - b. Expedited preservation and partial disclosure of traffic data
 - c. Production orders for computer data
 - d. Search and Seizure for computer data
 - e. Real-time collection of computer traffic data and

f. Interception of content data

Madam Chair, we are also of the view that adequate conditions and safeguards should be provided for under the future convention to ensure that these special investigatory powers and procedures are not abused, to ensure the protection of fundamental human rights and freedoms, including the right to privacy. Ghana has proposed text in that regard.

In conclusion, in the spirit of shaping the Convention to counter the use of ICT for criminal purposes, Ghana holds that the Convention should harmonise national laws on cybercrime, improve investigatory powers and procedures, and promote and enhance international cooperation. Further, it should extend into sustainable capacity building measures to enhance domestic capabilities and enable the sharing of good investigative practices and experiences.

I thank you for your kind attention.