African Union Cyber Security Experts Group (AUCSEG) under the auspices of the African Union Commission (AUC) input into the UN AdHoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.

Third Session, New York, 29 August – 09 September 2022.

Responses to Guiding Questions input into the UN AdHoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.

Third Session, New York, 29 August – 09 September 2022.

This contribution is not a collective African member states position but a position of the African Union Cyber Security Experts Group (AUCSEG) under the auspices of the African Union Commission (AUC).

It is without prejudice to the specific needs of sovereign nations across Africa.

The contribution is also without prejudice to any future contributions that AUCSEG may make during current and future discussions.

I. Provisions on International Cooperation

General Principles and Scope of the provisions on international cooperation

1. What forms of international cooperation should be stipulated in the convention? In addition to extradition, mutual legal assistance and law enforcement cooperation, should the convention cover transfer of sentenced persons; transfer of criminal proceedings; joint investigation; and international cooperation for the purposes of confiscation, and return and disposal of confiscated assets?

R **In addition to extradition, mutual legal assistance, and law enforcement cooperation we agree that international cooperation cover transfer of sentenced persons; transfer of criminal proceedings; joint investigation; and international cooperation for the purposes of confiscation, and return and disposal of confiscated assets, however such cooperation agenda must recognise state sovereignty and the limits within which external interference should be allowed for criminal proceedings.**

We suggest that the process of Mutual Legal Assistance Treaties (MLAT) needs to be reformed to enhance efficiency of transmission and responsiveness, noting that the continued advancement of innovative technologies demand that robust anticrime mechanisms are imperative.

2. What should be the scope of offences to which the international cooperation mechanisms stipulated in the convention apply? The proposals submitted by Member States indicate a common understanding that the extradition provisions would apply only to offences established in accordance with the convention. In relation to other forms of international cooperation such as mutual legal assistance, transfer of criminal proceedings and cooperation between law enforcement, should these provisions apply to the collection and sharing of electronic evidence for offences beyond those established in accordance with the convention? If so, should they apply regardless of the penalties for the offences where electronic evidence needs to be collected and shared, or should the scope be limited to "serious offences"?

3. Should the provisions on extradition and mutual legal assistance follow the models established by the United Nations Convention against Transnational Organized Crime or the United Nations Convention against Corruption, and, if so, to what extent?

4. Should the international cooperation provisions apply to the investigation and prosecution of civil and administrative cases related to the liability of legal persons for committing an offence established in accordance with the convention?

R **In line with the Article 30 of the African Union Convention on Cybersecurity and Personal Data Protection, the elaboration of the convention in relation to international cooperation provisions should apply in a manner that will allow State take the necessary legislative measures to ensure that legal persons other than the State, local communities and public institutions can be held responsiblefor the offences provided for by the Convention, committed on their behalf by their organs or representatives.**

5. Should the convention include a threshold penalty period for the offences to which the extradition article may apply (e.g., offences subject to a maximum penalty of not less than a given number of years of imprisonment)? We agree that to ensure consistency amongst states for the penalty administered over offences, the convention should

include threshold penalty for offences to which the extradition article may apply. This will also ensure that states do not abuse human rights in the guise of penalising offences.

R **It is imperative to ensure consistency amongst states for the penalty administered over offences, the convention should include threshold penalty for offences to which the extradition article may apply. This will also ensure that states do not abuse human rights in the guise of penalising offences.**

6. How can consistency be ensured between international cooperation provisions and the respect of human rights? A/AC.291/13 V.22-10829 3/6.

R **The Convention can ensure consistency between international cooperation provisions and the respect of human rights by building upon extant international law, which is already consistent on how states address international cooperation and human rights. We maintain that the Convention must be guided by international human right standards as set forth in the various international human rights documents, existing global commitments and further recognising the principle of necessity and proportionality.**

7. How should the chapter on international cooperation determine the requirements for the protection of personal data for the purposes of the convention?

R **We are of the opinion that a proper cybercrime statute must consider personal data protection for the investigation and prosecution of cybercrime. To ensure the respect of human rights, we agree that the chapter on international cooperation should make provisions for respect and protection of personal data to achieve the purposes of international cooperation for extradition, mutual legal assistance, and law enforcement. We refer to the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention) 2014, where the African Union Commission underscores personal data protection in the countering of cybercrime.**

Transmission of requests and materials

8. What channels for transmission of requests for extradition should be provided for in the convention?

9. What channels of transmission for mutual legal assistance requests should be provided for in the convention, in particular considering the nature of offences due to be covered by the convention?

10. What means of transmitting requests are needed to facilitate international cooperation, in particular considering the nature of offences due to be covered by the convention? Could requested documents or electronic evidence be transmitted by electronic means?

11. What key information would have to be submitted in a request for international cooperation under the convention? For example, should provisions set out the minimum information required?

12. What mechanism should the convention establish for handling mutual legal assistance or extradition in urgent circumstances? Should the International Criminal Police Organization (INTERPOL) channel be used? If so, how would urgent circumstances be defined? What kinds of request would be transmitted through the channel?

R **The International Criminal Police Organization (INTERPOL) and regional Criminal Police Organisations such as the African Police Cooperation Organisation (AFRIPOL) should be channels for handling mutual legal assistance because of their existing roles in coordinating international and regional law enforcement, including cybercrimes in recent times. In defining and determining what is urgent, the Committee is also reminded that in the cyber-domain, time is significantly compressed, and urgency may not necessarily be defined in terms of time limitation but impact. We therefor urge the committee to consider the definition of urgency in terms of the degree, scale, and associated dependencies of the effect of the crime in question.**

Grounds for refusal

13. Should the convention specify grounds for refusing an extradition request? If so, which grounds should be included for refusing the extradition? 14. Should the convention specify grounds for refusing a mutual legal assistance request? If so, which grounds should be included for refusing mutual legal assistance? 15. Should the

convention simply defer grounds for refusing an extradition or mutual legal assistance request to the domestic legislation of the State party and applicable treaties?

R **The convention should defer grounds for refusing an extradition or mutual legal assistance request to the domestic legislation of the State party and applicable extradition treaties between states recognising the circumstances of the cases and giving regard to extant criminal law and extradition agreements between states.**

16. Should the convention include a clause stating that the offences established in accordance with the convention shall not be considered a political offence, and that international cooperation shall not be rejected solely on those grounds?

R **It is not necessary to include a clause stating that the offences established in accordance with the convention shall not be considered a political offence. International cooperation must remain a matter of choice between sovereign states with due recognition to the degree and scale of the criminal activity in question. Political considerations are subjective and a convention that focuses on criminality need not necessarily include clauses clarifying political considerations.**

Other questions

17. Should the convention include specific provisions on mutual legal assistance regarding provisional measures? If so, what specific provisions should be included? For example, should they include the expedited preservation of stored computer data and electronic information, and expedited disclosure of preserved traffic data?

18. Should the convention include specific provisions on investigative powers? If so, what specific provisions should be included? For example, should they include access to stored computer data and electronic information, real-time collection of traffic data and interception of content data?

R **The convention must be clear on how member states establish measures to exercise powers and procedures necessary for the purpose of specific investigations or proceedings. This provision should refer to the collection and management of evidence in electronic form of the criminal offences established in Convention and in accordance with global good practices. The convention must also ensure that appropriate standards are stipulated for competent authorities in States to ensure the preservation and appropriate disclosure of data that has been stored by means of a computer system, where such data is relevant for investigation purposes.**

19. Should the convention include a provision on transborder access to [data] [information]? It would allow for a State to access stored [computer data] [electronic information] without the authorization of the State party where such [data are] [information is] geographically located, if the [data are] [information is] publicly available, or if access to the [data] [information] is through a computer system located in its territory and that State obtains the consent of the person who has lawful authority to disclose the [data] [information] through that computer system.

R **We are concerned that the more digitally advanced states may not fairly reciprocate with the less digitally developed nations in terms of accessing data stored within their jurisdictions. The convention must be clear on how member states establish measures to exercise powers and procedures necessary for the purpose of specific investigations or proceedings.**

We are concerned that digitally advanced states may restrict access to less digitally endowed States of stored [computer data] [electronic information] without the authorization of the State party where such [data are] [information is] geographically located, if the [data are] [information is] publicly available, or if access to the [data] [information] is through a computer system located in its territory and that State obtains the consent of the person who has lawful authority to disclose the [data] [information] through that computer system.

Furthermore, there are known instances where digitally advanced states consider their jurisdiction to encompass the service providers country of origin (registration) not the physical location of the data centre where the data resides.

If such provisions are included, they must be clear on equitable terms, recognising the differences and challenges between nation states. The convention to be clear on what "publicly available" means so that some states may not use such a provision as a basis to erode the sovereignty of other states, especially the digitally weaker states.

20. Should the convention include provisions to facilitate the return of assets? How should the convention address international cooperation for purposes of seizure and A/AC.291/13 4/6 V.22-10829 confiscation, and return and disposal, of confiscated assets, in particular as regards the difference between the approaches of the United Nations Convention against Transnational Organized Crime and the United Nations Convention against Corruption?

21. Should the convention include a provision for States parties to establish a 24/7 network of points of contact? What would be the purpose of such a network and its relationship with networks established under existing international instruments and frameworks?

R **In line with existing international and regional instruments such as the Budapest Convention and the Malabo Convention, there should be a provision for States parties to establish institutionally based 24/7 network of points of contact. The operation of the 24/7 points of contact should occur in conjunction to and with consideration of provisions of the convention; and states should establish regimes to provide mechanisms to ensure a single point of institutional contact for incidents and their resolution in international cooperation with other intragovernmental, law enforcement and sectoral efforts. This will ensure that states make use of existing means of international cooperation with a view to responding to cyber threats, improving cybercrime mitigation initiative, and stimulating dialogue between stakeholders. Institutional points of contact may be international, regional, intergovernmental, or based on private and public partnerships.**

22. Should the convention include a specific provision on international cooperation for carrying out electronic surveillance and other types of covert special investigative techniques, as part of cross-border [cybercrime] [criminal uses of information and communications technologies] investigations? 23. Should the convention include a provision permitting the organization of hearings held by video or telephone conference for the taking of evidence, and enabling such hearings to be conducted through the use of the requesting State's diplomatic missions and consular posts with respect to their own nationals on a voluntary basis, as part of consular functions.

II. Provisions on Technical assistance

24. Which specific areas of technical assistance should be covered by the convention?

R **Capacity development related to improving people, process and technology and related strategies of enhancing evidence sharing, judicial cooperation and assistance in criminal investigations and prosecutions that involve possible cybercrimes as defined in the convention. Improving and streamlining law enforcement's ability, in various jurisdictions, to obtain and exchange evidence needed for investigations and prosecutions and deepen the cooperation against terrorism and transnational organized crime, including cybercrime. Technical assistance support on infrastructure development for developing countries e.g., Computer Emergency Response Teams (CERTs). Enhancing relations by affording nations with improved information-sharing; creating regularised and streamlined channels for obtaining law enforcement assistance. Better enabling prosecutors to exchange information facilitating the prevention, investigation, and prosecution of crime.**

25. Which principles should be used to guide technical assistance and capacity-building efforts? Should these include drawing on best practices? How can the convention ensure such assistance takes into consideration a gender perspective?

R **Respect for persons; State sovereignty; Eventual self-sustainability of outcomes; Systematically align the goals of technical assistance programs with those of the beneficiary nations state (s); Effective monitoring and feedback mechanisms to determine and predict program participants' needs; and provide meaningful training through opportunities to apply learning. Offering multiple technical assistance strategies with levels of support including utilising effective learning strategies; developing trusting relationships; encouraging feedback loops and broad-based benefits.**

26. What are the specific needs of developing countries in countering the use of information and communications technologies for criminal purposes and how could they be addressed in the technical assistance chapter of the convention?

R **States must be encouraged to generate the needed human resources pipelines for cyber-professional by designing and implementing the appropriate curricular at "national" anti-crime training institutions and across academia. It is therefore recommended, that it is necessary to establish and enhance capacity at regional, national, and sub-national levels across the global south, and Africa in particular. Country specific, strategic, and sustainable capacity building is required given the varied anti-cybercrime maturity levels, local context, political realities, and cultural diversity.**

Institutions require capability for developing and sharing research methodologies and statistics for anti-cybercrime needs and readiness assessments at national, sub-regional and regional level. This will include conducting comprehensive national cyber-needs assessments to determine gaps and needs of the different actors and stakeholder groups participating in counter cybercrime processes.

Capacity development for the protection of Critical Infrastructure (CI) and Critical Information Infrastructure (CII) is needed, because CI and CII can be negatively impacted by criminals. This includes enhanced capacity for effective communication among response teams, between them, and with other stakeholders. Technical assistance support on infrastructure development like Computer Emergency Response Teams (CERTs), specialised cybercrime investigative capacities, and national cybercrime prosecution Units. It is important to assist African states to establish national and sectoral CSIRTs and CERTs where they are not yet in place. It is important to also develop and implement mechanisms for national, sub-regional, regional, and continental collaboration between Cybersecurity Incidents Response Teams (CSIRTs), Computer Emergency Response Teams (CERTs), or equivalents. This includes enhanced capacity for effective communication among response teams, between them, and with other stakeholders. Technical assistance support on infrastructure development like Computer Emergency Response Teams (CERTs), specialised cybercrime investigative capacities, and national cybercrime prosecution Units.

The convention should encourage initiatives that support and empower women with equitable opportunities and programs in countering the use of information and communications technologies for criminal purposes.

Global Cyber health and hygiene protection platform with an Early Warning System (EWS) that conducts critical research and provides cyber related information that protects all of us from expensive and dangerous cyber threats and empowers authorities to respond when they arise.

27. Should the convention include provisions on the specific roles of the United Nations Office on Drugs and Crime (UNODC)? Should it also include provisions on the role of INTERPOL and other relevant international bodies and organizations?

R **The convention should support the development of a transparent and efficient accreditation mechanism coordinated by either the UNODC or Interpol that can grow or shrink based on international affiliates adhering to the standards of implementation of the convention.**

28. Which methods and means of providing technical assistance should be covered by the convention?

R **The convention should seek to enhance the credibility of relevant institutional with and between nation states; support the professional development operatives, encourage related coaching & mentoring programs, provide technical consultation, and encourage multi stakeholder support and feedback processes.**

29. Why do some States use the term "technical assistance" and others "capacity-building"? What is the difference between them? Should the convention include provisions on capacity-building? If so, what should they entail?

R **Technical assistance a process that facilitates the provisioning of support to an entity towards bridging research, policy, and practice gaps. Such support may encompass capacity building, which the development of skills, process, and related technology to improve the performance of an entity.**

The convention should include provisions on capacity-building that may include but not be limited to collaboration of various platform development, awareness raising and raising security culture; workforce progression and enhancement; gender equity initiatives; collection, development, analysis, and publication of statistical information in support of decision making; and incentives to discourage digital authoritarian tendencies.

30. Should the convention include provisions that are aimed at assisting States parties with resources for a 24/7 point of contact?

R **The Convention should include measures to promote, and possibly initiate, self-sustaining mechanisms for institutional 24/7 point of contact's based with the national coordinating Computer Emergency Response Team or equivalent.**

31. What, if any, could be the role of the private sector and non-governmental organizations in technical assistance or capacity-building

R **The convention should encourage programs that leverage Civil Society to foster good governance of public and private sectors.**

States can use multilateral, regional, bilateral, and multi-stakeholder platforms to exchange practices and share information on national approaches to combatting cybercrime. Promoting common understandings and mutual learning can also strengthen international cooperation and assistance in the area of ICT security and capacity-building. An often-ignored sector for capacity building in Africa is the civil society groups. Cybercrime responses especially for Africa must transcend the traditional notions of security. While governments play the primary role in creating the public policies and laws that regulate and determine cybercrime measures domestically, it is important to build capacity for African Civil societies so that Africa can leverage multistakeholder partnerships in line with Article 26 of the African Union Convention for Cybersecurity and Personal Data Protection (Malabo Convention) 2014.

Civil society is uniquely positioned to advocate for policies based on a human rights approach and can play an important role by monitoring and documenting government and business practices, identifying knowledge gaps, and providing analysis to inform policies and relevant discussions.

Private sector and non-governmental organizations, as well as professional organizations, such as AfricaCERT, can play a central role in supporting the realisation of trusted cyber environment, as well as in supporting and empowering African countries in capacity building and awareness raising.

Confronting emerging cyberthreats and cybercrimes requires sincere, coherent, and sustained efforts, as well as extensive and comprehensive worldwide partnerships, involving governments, international organizations, private sector, research and educational institutions, media, business organizations and civil society; in order to raise awareness towards maximizing the benefits of the unique opportunities offered by advanced information and communications technologies in various economic, social and cultural domains, while protecting our society from the risks of cybercrimes and cyberattacks.

The reality of cybercrime often collides with realties of developing states, particularly for states in the African region which are at the lower end of the digital divide and lack the capacity, skills and infrastructure to effectively combat cybercrime at international standards. Law enforcement institutions need capacity building strategies that underscore effective collaboration, mutual legal assistance, and the understanding that the prosecution of cybercrime requires the respect of human rights in cybercrime policing strategies. Policy makers, Diplomats, Parliamentarians and other strategic decision makers need capacity development to understand the cybercrime landscape, actors and the involvement of multi-stakeholder groups in shaping appropriate and effective policies which consider good practice. Capacity building is also relevant for the judiciary for understanding, addressing cybercriminal matters, and issues of applicability of electronic evidence and related matters.

It is vital to consistently build capacity for understanding the threat landscape across Africa. The achievement of this goal hinges on overcoming many challenges. African states' under-resourced institutions which often lack the technical skills, managerial capacities, and financial resources to effectively articulate and implement cyber policies, and related enforcement measures. Developing a regional cybercrime centre like other regions to enhance cross-border cooperation and information sharing will enhance capacity building efforts for countering cybercrime in the region.

III. Provisions on Preventive measures

32. On which areas should the chapter on preventive measures focus? Are there particular groups, such as children, for whom preventive measures would need to be prioritized?

R **We have seen that children, women, and the elderly as targets groups for cyber-criminal activities generally due to awareness and digital literacy it is important that preventive measures are prioritised for such groups. Beyond making provisions towards preventive measures for vulnerable groups such as children and women, the convention should also make provisions for the assistance to and protection of victims by ensuring that states take appropriate measures to provide assistance and protection to victims of offences covered by the Convention. This is in line with Article 25 UNTOC. This is also an area that should be considered as a technical assistance objective including international cooperation broadly.**

The convention should also encourage the establishment of early warning and detection systems.

33. How should Member States prevent cyber-criminal attacks targeting critical infrastructures?

R **Member States are encouraged to foster enhanced cyber-culture across society; invest in basic cyber-hygiene as a foundational defence; minimise single points of institutional and technical failure.**

34. In which areas would the convention require that States parties take measures to cooperate with civil society, the private sector and academia, with a view to preventing the use of information and communications technologies for criminal purposes?

R **States must promote at multilateral levels, the consideration of existing and potential cybercrime threats, as well as possible strategies to address the such emerging threats, consistent with the need to preserve the free flow of information to preventing the use of information and communications technologies for criminal purposes**

The convention should require states to leverage multistakeholder mechanisms to develop, implement, monitor standards and compliance. Provisions in the convention should require States to enact domestic legislation that provide guidance on preventing cybercrimes and enhancing the resilience of institutions in the areas of Organisational Readiness, Situational Awareness, Cyber Defence, Detection, Mitigation and Containment, and Recovery through a multistakeholder approach.

As we consider the stakeholders, we need to appreciate their value proposition for the implementation of the convention, namely:

- **The Private sector owns much of the infrastructure and platforms.**
- **Academia provides the teaching, learning, research, and development needed to enhance an anti-cybercrime culture and support development.**
- **Innovators take the output of Research and Development to market as new technological products and services.**
- **Media will enhance a culture of accountability and promote awareness initiatives.**
- **Civil society is adept at holding the public and private sectors accountable. Civil society is uniquely positioned to advocate for cybercrime policies based on a human rights approach and can play an important role by monitoring and evaluating government initiatives and business practices, identifying knowledge gaps, and providing analysis to inform policies and relevant discussions.**
- **Government has statutory duties to provide clear and fair operating regimes and deterrence, towards ensuring optimal stakeholder partnerships.**

35. Should the convention provide for the designation of a national authority responsible for preventing the use of information and communications technologies for criminal purposes?

R **Without being very prescriptive, the convention should provide for the designation of a national authority responsible for preventing the use of information and communications technologies for criminal purposes. This aligns with the African Union (Malabo) Convention on Cybersecurity and Personal Data Protection 2014 Articles 24 and 25 which provides for measures to be taken at National Level, including the establishment of related National regulatory bodies. The Malabo Convention further mandates states in Article 27 to establish national monitoring structures, including an institutional framework and the adoption of the necessary measures to establish an appropriate institutional mechanism responsible for governance of anti-cybercrime activities.**

36. Should the convention include a provision requiring States parties to create responsibilities for the private sector to establish and implement standards that are aimed at enhancing measures to prevent criminal uses of information and communications technologies? Should the convention include provisions that are aimed at harmonizing domestic legislation in that regard, in order to provide clear guidance for the private sector to prevent crime?

R **The creation of responsibilities for private sector should be a matter left for national considerations. However, the convention should include a provision**

setting out minimum benchmarks and requiring States parties to create responsibilities for, and participation of, the private sector, and other providers, to establish and implement standards that are aimed at enhancing measures to prevent criminal uses of information and communications technologies. This will enhance clarity and the monitoring of implementation of public-private partnership. It is important that in the overall achievement of the objectives of the convention that it includes provisions that are aimed at the harmonisation of laws across borders to facilitate the implementation of the convention.

37. How should the convention encourage States parties to raise awareness of the threat of [cybercrime] [criminal uses of information and communications technologies] and encourage companies, organizations and individuals to take action that will make them more resilient to [cybercrime] [criminal uses of information and communications technologies]?

R **The convention should encourage States parties to raise awareness of the threat of cybercrime, criminal uses of information and communications technologies and encourage companies, organizations, and individuals to act through including a provision on a national anti-cybercrime system – requisite leadership and culture. This is in line with the African Union Convention on Cybersecurity and Personal Data Protection 2014 Article 26.**

Capacity development towards leveraging the exiting features than can be transformed into capabilities should be encouraged. It is vital to advance a culture of combating cybercrime leadership for example in Africa. It will be beneficial if adequate resourcing for countering cybercrime capacity development for citizens through skills development, education and awareness is given adequate attention, including through integrating basic cybercrime prevention education into curricula at schools and institutions.

IV. Provisions on Mechanism of implementation

Cybercriminals operate at the speed of light, while Law Enforcement operates at the seed of law. Therefore, we advocate that the convention should have mechanisms for its evolution in the dynamic environment that it will exist in. This also informs our earlier stated opinion that the MLAT process needs enhancement.

38. What mechanisms of implementation of the convention should be provided for in the convention?

39. What is the most acceptable option, from the following, for the drafting of the chapter on the mechanism of implementation:

(a) A structure similar to that established by the United Nations Convention against Transnational Organized Crime or the United Nations Convention against Corruption, namely, the mechanism of a Conference of Parties;

(b) A structure similar to that established for the implementation of the three international drug control conventions, namely, the Single Convention on Narcotic Drugs of 1961, as amended by the 1972 Protocol, the Convention on Psychotropic Substances of 1971 and the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988, which entrusts the Commission on Narcotic Drugs and the International Narcotics Control Board to follow up on convention implementation? For example, implementation of the convention could be considered by the Commission on Crime Prevention and Criminal Justice and be focused on targeted periodic reviews of implementation, as well as under an annual agenda item for the Commission on Crime Prevention and Criminal Justice;

(c) The establishment of a specific body for the review of the implementation of the convention, either independently or under a Conference of Parties (similar to the structure of the Committee on the Peaceful Uses of Outer Space, which has a Scientific and Technical Subcommittee)?

R **We are inclined to option (b), as Mechanisms and structures for implementation of the convention can be patterned like that established for the implementation of the three international drug control conventions, in a manner that entrusts a**

Commission to follow up on convention implementation. The conventions include: the Single Convention on Narcotic Drugs of 1961, as amended by the 1972; Protocol, the Convention on Psychotropic Substances of 1971; and the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988. However, such a commission must provide for a number of seats on rotational elective basis to allow the expertise of relevant non-governmental organizations, civil society organizations, academic institutions and the private sector to cover equitable geographical representation.

40. How can the convention ensure that the implementation mechanism makes best use of the experience and expertise of relevant non-governmental organizations, civil society organizations, academic institutions and the private sector?

R **The Commission as suggested in question 39 (b), must provide for a number of seats on rotational elective basis to allow the expertise of relevant non-governmental organizations, civil society organizations, academic institutions and the private sector to cover equitable geographical representation.**

V. Final provisions

41. Should the convention include a provision on the effects of the convention with a view to defining the relationship of the convention with other treaties, agreements or arrangements on matters dealt with in the convention?

R **We agree that the convention should include a provision on the effects of the convention with a view to defining the relationship of the convention with other treaties, agreements or arrangements on matters dealt with in the convention.**

42. Should the convention include a provision on the development of additional or supplementary protocols and their relationship with the convention? If so, what should be the nature of the mandated body and procedure for the elaboration and adoption of protocols to the convention?

R **The convention should include a provision on the development of additional or supplementary protocols and detail their relationship with the convention.**

43. Should the convention allow for reservations by States parties, and, if so, what should be the limitations to such reservations?

R **The convention should allow for reservations, especially considering that some developing countries are still at a cybercrime legislation development stage, and this reality means that certain provisions may not be realisable or achievable for such countries.**

44. What dispute settlement mechanism should the convention provide for?

45. What should be the number of necessary ratifications by States parties for the entry into force of the convention? How many days should pass after the deposit of the last required instrument of ratification or accession before the entry into force of the convention?

R **This should be decided similarly to the United Nations Convention against Transnational Crime and its Protocols; hence, the Convention should enter into force on the ninetieth day after the date of deposit of fifty-eight (30% of UN members states) or more instruments of ratification. We also ask that the basis of entry into force and the demanded ratifications should be decided in a manner that considers equitable geographical balance of ratifications before the convention enters into force.**

46. Should the convention allow for amendments and, if so, what procedure should be foreseen?

R **The convention must allow for amendments, and we propose a similar amendment procedure to the procedure stipulated in the African Union**

Convention on Cybersecurity and Personal Data Protection 2014. Any State Party may submit proposals for the amendment or revision of the Convention. Proposals for amendment or revision should be submitted to the Chairperson of the convention implementation monitoring office who shall transmit same to State Parties within thirty (30) days of receipt thereof; an assembly of states shall consider the proposals provided all State Parties have been given adequate notification before the beginning of the session. A rules of amendments procedure must also be developed alongside the development of the convention to allow the states to adopt amendments in accordance with such rules of procedure.

VI. Preamble

47. What principles and main elements should be included in the preamble?

48. Do Member States agree to waiting until progress has been made on the substantive articles of the convention before drafting the content of the preamble?

R **It will serve a better purpose to wait until adequate progress has been made on the substantive articles of the convention before drafting the content of the preamble.**

African Union Cyber Security Experts Group (AUCSEG)
under the auspices of the
African Union Commission (AUC)