20 April 2022

English only

Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes
Second session
Vienna, 30 May–10 June 2022

Overview of existing instruments, recommendations and other documents on countering the use of information and communications technologies for criminal purposes

Note by the Secretariat

Summary

The present conference room paper has been prepared by the Chair of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, to facilitate consideration by the Ad Hoc Committee of existing international instruments and efforts at the regional and international levels on combating the use of information and communications technologies for criminal purposes, as mandated by the General Assembly in paragraphs 2 and 11 of its resolutions 74/247 and 75/282, respectively. The text provides an overview of those instruments, recommendations and other documents aimed at countering the use of information and communications technologies for criminal purposes, and presents, inter alia, a list of provisions of international legally binding instruments on this matter.

V.22-02403 (E)

Overview of Existing Instruments, Recommendations and other Documents on Countering the Use of Information and Communications Technologies for Criminal Purposes[1]

Contents

[1] The terms “cybercrime” and “use of information and communications technologies for criminal purposes” have been used interchangeably throughout this document.

I. Introduction

This text provides an overview of global, regional and other multilateral efforts aimed at countering the use of information and communications technologies (ICTs) for criminal purposes and presents a list of provisions of international legally binding instruments on this matter, under different thematic sub-headings. It was prepared by the Chair of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, with the assistance of the secretariat, to facilitate deliberations of the Committee.

Furthermore, the paper contributes to the implementation of paragraphs 2 and 11 of General Assembly resolutions 74/247 and 75/282, respectively, in which the Assembly reaffirmed that the Ad Hoc Committee shall take into full consideration existing international instruments and efforts at the national, regional and international levels on combating the use of information and communications technologies for criminal purposes, in particular the work and outcomes of the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime (Cybercrime IEG). This paper only considers information that is publicly available and open-source.

The document consists of two substantive sections. Section II provides an overview of existing global, regional and other multilateral instruments, recommendations and other documents on countering the use of ICTs for criminal purposes.[2] Moreover, in this Section, the paper considers model legislation developed at subregional level, to reflect initiatives at various regions, given that relevant legally binding instruments are not evenly distributed in the world.

Section III presents provisions of multilateral legally binding instruments on the use of ICTs for criminal purposes covered in Section II, and recommendations of the Cybercrime IEG, as appropriate, which may be referenced during the elaboration of the new convention. The provisions were organized under specific categories, such as “Statement of Purpose”, “Scope of Application”, or “Definitions”. Some of the provisions contained in the United Nations Convention against Transnational Organized Crime (UNTOC) and the United Nations Convention against Corruption (UNCAC) were included, where they addressed the same or similar subjects (e.g. on the definition of confiscation, see further below at Section III.B.5). In addition, the recommendations of the cybercrime IEG were also included when they were relevant to specific categories, as required by General Assembly resolutions 74/247 and 75/282.

II. Overview of International Instruments, Recommendations and Other Documents on Countering the Use of Information and Communications Technologies for Criminal Purposes

A. United Nations

1. United Nations Convention against Corruption

The United Nations Convention against Corruption (UNCAC)[3] is a globally binding convention with the aim of preventing and combatting corruption, promoting international cooperation and technical assistance in this regard, including in asset

[2] The following methodology has been applied for the order of the instruments and documents in Section II: United Nations instruments and documents are listed first, followed by legally binding agreements, directives issued by regional organizations, and model legislative provisions prepared by regional organizations. The instruments and documents were listed in alphabetical order within their respective categories.

[3] See http://www.unodc.org/unodc/de/treaties/CAC/.

recovery, and promoting integrity, accountability and proper management of public affairs and public property. It entered into force on 14 December 2005. It has 189 States parties as of March 2022. The Convention covers six main areas: preventive measures, criminalization and law enforcement, international cooperation, asset recovery, technical assistance and information exchange, and mechanisms for implementation. A unique feature of the Convention is the inclusion of a chapter on asset recovery, aimed at returning assets to their rightful owners, including countries from which they had been taken illicitly.

UNCAC does not specifically concern cybercrime. Nevertheless, the following provisions might still be useful in the negotiation of a new convention on countering the use of ICTs for criminal purposes: liability of legal persons (art. 26), ancillary provisions on criminalization (arts. 27-30), freezing, seizure and confiscation (art. 31), protection of witnesses, experts, victims and reporting persons (arts. 32-33), provisions related to law enforcement (arts. 36-39), criminal record (art. 41), jurisdiction (art. 42), international cooperation (chapter IV), asset recovery (chapter V), technical assistance and information exchange (chapter VI), mechanisms for implementation (chapter VII), and final provisions (chapter VIII).

2. United Nations Convention against Transnational Organized Crime

The United Nations Convention against Transnational Organized Crime (UNTOC) is the only global legally binding instrument to combat transnational organized crime. It entered into force on 29 September 2003, and with 190 States parties it has achieved almost universal adherence. It was supplemented by three protocols, which contain provisions on combating specific forms of organized crime: The Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, the Protocol against the Smuggling of Migrants by Land, Sea and Air and the Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition.

While UNTOC does not specifically concern cybercrime, it may nevertheless apply to ICT-related crimes if the particular crime falls within the scope of application stipulated in article 3 of the Convention.

In addition, as a recently developed criminal law convention, some of its provisions could be useful in the elaboration of a new convention on countering the use of ICTs for criminal purposes. For example, provisions on the liability of legal persons (art. 10), prosecution, adjudication and sanctions (arts. 11), international cooperation provisions such as international cooperation for the purpose of confiscation, joint investigation, training and technical assistance (art. 29), the implementation of the convention (arts. 30, 34), and final provisions (arts. 35-41) could be used as reference for the new convention.

3. The 2021 GGE and OEWG Reports

The 2021 GGE and OEWG reports are important non-binding intergovernmental reports on the impact of new technology on international security. The 2019-2021 *Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security* (OEWG) was established by the General Assembly in its resolution 73/27.[4] The OEWG's mandate was to develop further rules, norms and principles of responsible state behaviour, study the possibility of establishing a regular institutional dialogue under auspices of the United Nations, continue to study existing and potential threats in the sphere of information security, how international law applies to the use of ICTs by states, as well as confidence-building and capacity-building measures in this field, and to submit a

[4] Available at https://undocs.org/A/RES/73/27.

report on the results to the General Assembly.[5] The OEWG delivered its report in March 2021.[6]

The 2019-2021 *Group of Governmental Experts on advancing responsible state behaviour in cyberspace in the context of international security* (GGE), on the other hand, was established by the General Assembly in its resolution 73/266.[7] Similarly to the OEWG, the GGE's mandate was to continue to study measures to address existing and potential threats in the information security sphere, norms, rules and principles of responsible state behaviour, confidence-building and capacity-building measures, as well as how international law applies to the use of ICTs by States, and to submit a report of the result to the General Assembly.[8] It is the 6th GGE of this kind established under the auspices of the United Nations.

As a result of deliberations within the six GGEs with comparable mandates, four reports were produced, in 2010, 2013, 2015, and 2021. The GGE of 2019-2021 delivered its report in May 2021.[9] The GGE report of 2015 is considered to be one of the most important reports of the GGE, as it – for the first time – established so-called voluntary, non-binding norms of responsible state behaviour in cyberspace.

The GGEs are limited to only a number of states (the GGE of 2021, e.g., was limited to 25 member states), representative of all geographical regions. The OEWG of 2019-2021 was open to all member states.

While the OEWG report was more general in scope, describing overall issues in the context of new technology and international security, the GGE focused on the implementation of the already existing voluntary non-binding norms of responsible state behaviour, established by the GGE report of 2015.[10]

Relevant for the cybercrime context, voluntary non-binding norm 13d) of the 2015 GGE report notes that *"States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect."*

The 2021 GGE report further clarifies the content of norm 13d), noting that the primary focus of this norm is to strengthen international cooperation. States are encouraged to strengthen existing mechanisms, but also to "*develop appropriate protocols and procedures for collecting, handling and storing online evidence relevant to criminal and terrorist use of ICTs and provide assistance in investigations in a timely manner, ensuring that such actions are taken in accordance with a State's obligations under international law*".[11]

Moreover, it refers to the already existing international fora, processes and resolutions dedicated to the criminal aspects of cybersecurity,[12] and encourages states to develop partnerships with other stakeholders.[13]

During the negotiations in the OEWG, it became clear that especially developing countries were concerned about the increasing threat of cybercrime to international security. In that context, the OEWG report notes that "[t]*he continuing increase in incidents involving the malicious use of ICTs by State and non-State actors, including*

[5] GA resolution 73/27, paragraph 5.
[6] The full report is available at https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.
[7] Available at https://undocs.org/en/A/RES/73/266.
[8] GA resolution 73/266, paragraph 3.
[9] The full report is available at https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf.
[10] The full report is available at https://undocs.org/A/70/174.
[11] 2021 GGE report, paragraph 33.
[12] Ibid., paragraph 34.
[13] Ibid., paragraph 35.

terrorists and criminal groups, is a disturbing trend. Some non-State actors have demonstrated ICT capabilities previously only available to States."[14]

While both reports are non-binding, they stress the importance of dealing with this transnational threat, in particular through fostering international cooperation.

4. The IEG Recommendations

In April 2021, the Intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime agreed on recommendations ('IEG Recommendations' or 'Recommendations') on how best to address issues of cybercrime through the implementation of legislation and frameworks on effective criminalization, law enforcement and investigation, electronic evidence and criminal justice, international cooperation, and prevention.[15]

The Recommendations emphasize the importance of the need for consistent terminology.[16] They also recommend that States "ensure that their legislative provisions withstand the test of time with regard to future developments in technology by enacting laws with formulations that are technologically neutral and criminalize the activity deemed illegal instead of the means used".[17]

The Recommendations further note that some crimes, which traditionally were committed "offline" (without cyber means), could also be committed *with* cyber means (so-called "cyber-enabled" crimes).[18] For such crimes, the existing national and international provisions, which cover "offline" crimes, should be used.

The Recommendations also suggest that States should be able to exchange information timely and securely, such as through a 24/7 Network.[19] In general, States are asked to strengthen existing networks, for exchanging information, best practices and evidence, and also to rely on INTERPOL channels, and make use of such networks before formally requesting mutual legal assistance (MLA).[20]

The Recommendations, at various places, emphasize the importance of effective international cooperation.[21] They stress the importance of having national laws in place which authorize or enable States to cooperate internationally.[22] They further emphasize the importance of international cooperation with respect to the sharing of electronic evidence.[23] Moreover, they support the establishment of rapid response mechanisms and direct channels of communication through liaison officers.[24] Also, States are encouraged to establish joint investigative teams.[25]

The Recommendations further suggest that national laws should be put in place which ensure the real-time collection of traffic data and content.[26]

Moreover, they contain a couple of provisions on mutual legal assistance. For example, they suggest that there should be the possibility to transmit MLA requests through electronic means to reduce delays and ensure fast and effective responses to

---

[14] 2021 OEWG report, paragraph 16, available at https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

[15] See Annex of the *Report on the Meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 6 to 8 April 2021*, 'Conclusions and Recommendations Agreed Upon by the Expert Group for Consideration by the Commission on Crime Prevention and Criminal Justice' (19 April 2021), UNODC/CCPCJ/EG.4/2021/2, available at https://undocs.org/en/UNODC/CCPCJ/EG.4/2021/2.

[16] Recommendations, paragraph 1.

[17] Ibid.

[18] Recommendations, paragraph 4.

[19] Ibid., paragraphs 6, 23 and 24.

[20] Ibid., paragraphs 13 and 23.

[21] Ibid., paragraphs 10, 17, 18, 37 and 56.

[22] Ibid., paragraphs 10 and 28.

[23] Ibid., paragraphs 18 and 30.

[24] Ibid., paragraphs 19 and 20.

[25] Ibid., paragraph 27.

[26] Ibid., paragraph 10 (a).

such requests.[27] They further note that countries may benefit from UNODC's MLA Request Writer Tool, which helps practitioners draft requests.[28] Moreover, they suggest that States may consider having specialized MLA cybercrime units (next to other specialized cybercrime forces),[29] keep databases for MLA requests[30] and to use central authorities for the transmission of requests.[31]

The recommendations also suggest that States should consider enacting legislation that ensures the collection, preservation, authentication and admissibility of electronic evidence.[32] Furthermore, it is recommended that States consider establishing traffic data, content data, subscriber data, and other "digital" data used for the commission of a crime as electronic evidence in their domestic laws.

A range of the recommendations also stress the importance of capacity-building measures. This includes the crucial work of UNODC in this field.[33] Moreover, many provisions stress the importance of strengthening the capacity of practitioners, in particular law enforcement officers, to deal with issues of cybercrime.[34] The recommendations further suggest training, networking and joint meetings for law enforcement officers, central authorities and lawyers to adjudicate cases.[35] It was also emphasized that especially developing countries may need more support for capacity-building than other countries.[36]

The recommendations also emphasize the role of the private sector in cybercrime, as a partner in raising awareness of cybercrime[37] and helping to prevent it,[38] but also as a victim of cyber operations.[39] They emphasize the importance of cooperation with businesses in general,[40] but also in particular with service providers.[41]

The recommendations also suggest allowing the public easy access to prevention tools (such as online platforms, infographics etc).[42]

The recommendations further emphasize that prevention efforts should focus on proactive measures, including awareness-raising, and disrupting ongoing illicit online activities.[43]

The recommendations further emphasize the need to protect vulnerable groups from cybercrime with suitable measures. States should thus work on preventing and eradicating gender-based violence,[44] consider efforts to protect children online, as well as to address hate crime and cyberbullying.[45] In that context, it is also recommended to involve female experts in the prevention and investigation of cybercrime.[46] Also, States should develop and strengthen victim support programmes.[47]

The importance of the protection of human rights is emphasized throughout the recommendations.[48] In particular, States should consider the proportionality of

[27] Ibid., paragraphs 25 and 30.
[28] Ibid., paragraph 32.
[29] Ibid., paragraphs 34 and 35.
[30] Ibid., paragraph 36.
[31] Ibid., paragraph 37.
[32] Ibid., paragraphs 12 and 17.
[33] Ibid., paragraphs 3, 7 and 31.
[34] Ibid., paragraphs 11 and 18(f).
[35] Ibid., paragraphs 29, 43 and 62.
[36] Ibid., paragraphs. 46 and 51.
[37] Ibid., paragraph 54.
[38] Ibid., paragraphs 38, 45 and 57.
[39] Ibid., paragraph 53.
[40] Ibid., paragraph 2.
[41] Ibid., paragraphs 18(d) and 22.
[42] Ibid., paragraph 39.
[43] Ibid., paragraphs 44 and 48.
[44] Ibid., paragraphs 41 and 42.
[45] Ibid., paragraphs 41 and 61.
[46] Ibid., paragraph 59.
[47] Ibid., paragraph 52.
[48] Ibid., paragraphs 17 and 50.

investigative measures and ensure that these measures respect fundamental freedoms and the right to privacy (including data protection).[49]

The recommendations further suggest the establishment of repositories, which, inter alia, facilitate the collection of data on trends to be able to build better policies on cybercrime.[50] Regular advisories should be issued and shared with the relevant audience to help in preventing further cybercrime.[51] Research should also be undertaken on the modi operandi of cybercriminals.[52]

B. African Union (AU)

The African Union Convention on Cyber Security and Personal Data Protection (also called 'Malabo Convention')[53] covers a wide range of aspects related to cybercrime. It was adopted on 27 June 2014, and has not yet entered into force, as it has not achieved the required numbers of ratification (see art. 36 AU Convention 2014, requiring 15 instruments of ratification; so far, 8 States have ratified the Convention).[54]

The Convention was drafted in 2011 to establish a "credible framework for cybersecurity in Africa through organization of electronic transactions, protection of personal data, promotion of cyber security, e-governance and combatting cybercrime."[55]

The AU Convention addresses three main areas: electronic transactions, personal data protection, and cybersecurity and cybercrime. Provisions related to cybercrime can be found particularly in article 25, paragraph 1, obligating States to establish national legislation on specific criminal offences; article 27, paragraph 2, on establishing appropriate institutions to combat cybercrime, article 28, on international cooperation, and Section II, which lays down the specific offences to be criminalized, and other relevant provisions.

C. Commonwealth of Independent States

The Commonwealth of Independent States Agreement on Cooperation in Combating Crimes in the Field of Computer Information (also referred to as the Minsk Agreement) was adopted on 1 June 2001 and entered into force on 14 March 2002. It focuses on strengthening cooperation between member States of the Commonwealth of Independent States to ensure the effective prevention, detection, suppression, uncovering and investigation of offences relating to computer information.

Subsequently, an Agreement on Cooperation in the Fight Against Crimes in the Field of Information Technologies (also referred to as the 'Dushanbe Agreement') was adopted on 28 September 2018, and entered into force on 12 March 2020. According to article 17 paragraph 2 of this Agreement, it shall replace the Minsk Agreement from the date of its entry into force. So far, five countries have ratified the Dushanbe Agreement. For the countries that have not yet ratified the Dushanbe Agreement, the Minsk Agreement remains in force.

In terms of scope of application, the Dushanbe Agreement is *broader, including, inter alia, further provisions on criminalization. In terms of str*ucture, the Dushanbe Agreement first defines key terms (article 1), specifies its objectives (article 2), and

[49] Ibid., paragraph 21.
[50] Ibid., paragraphs 49 and 60.
[51] Ibid., paragraph 58.
[52] Ibid., paragraph 55.
[53] Available at https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.
[54] As of June 2020, as per information available at https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf.
[55] See information available at: https://ccdcoe.org/organisations/au/.

subsequently describes punishable acts (article 3). Further, it contains provisions on competent authorities (article 4), forms of cooperation (article 5), mutual (legal) assistance (articles 6 to 11), and final provisions (articles 12 to 18).

D. Council of Europe (CoE)

The Council of Europe Convention on Cybercrime ("Budapest Convention", or "BC") was adopted on 23 November 2001 and entered into force on 1 July 2004. So far, 66 States have ratified it and further 11 States have signed it or been invited to accede to it.

The principal objectives of the Convention are to harmonize national legal frameworks, support cybercrime investigations, and enhance international cooperation to combat cybercrime. The Convention is divided into four chapters: use of terms (chapter I), measures to be taken at the national level (chapter II), international cooperation (chapter III), and final provisions (chapter IV).

There are two additional protocols to the Convention. The first additional protocol deals with the criminalization of acts of a racist and xenophobic nature committed through computer systems.[56] So far, 33 States have ratified the first additional protocol, which entered into force on 1 March 2006. The second additional protocol, which was adopted on 17 November 2021, addresses enhanced cooperation and disclosure of electronic evidence.[57]

E. League of Arab States

The League of Arab States has adopted a Convention on Combating Information Technology Offences in 2010. The Convention has entered into force on 7 February 2014, after its ratification by seven members of the League of Arab States.[58]

Its purpose is to strengthen cooperation between States within the League of Arab States to enable them to defend against and protect the States' property, people and interests from cybercrime. The Convention is exclusive to members of the League. The Convention contains chapters on general provisions (chapter I), procedural provisions (chapter III), legal and judicial cooperation (chapter IV), and final provisions (chapter V).

F. Shanghai Cooperation Organization (SCO)

On 16 June 2009, the Shanghai Cooperation Organization adopted the Agreement on Cooperation in the Field of International Information Security.[59] The agreement creates a legal and organizational basis for cooperation between the Parties in the field of international information security, including in 1) coordinating and implementing necessary joint measures in the field of ensuring international information security; 2) creating a system of joint monitoring and response to emerging threats in this area; and 3) elaborating joint measures for the development of international law provisions limiting the spread and use of information weapons threatening defence capacity, national security and public safety.

---

[56] Available at https://rm.coe.int/168008160f.

[57] Available at https://rm.coe.int/1680a49dab.

[58] Available at http://www.lasportal.org/ar/legalnetwork/Documents/%D8%A7%D9%84%D8%AA%D8%B5%D8%AF%D9%8A%D9%82%20%D8%B9%D9%84%D9%89%20%D8%A7%D9%84%D8%A7%D8%AA%D9%81%D8%A7%D9%82%D9%8A%D8%A9%20%D8%A7%D9%84%D8%B9%D8%B1%D8%A8%D9%8A%D8%A9%20%D9%84%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9%20%D8%AC%D8%B1%D8%A7%D8%A6%D9%85%20%D8%AA%D9%82%D9%86%D9%8A%D8%A9%20%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA.pdf.

[59] Available at: http://eng.sectsco.org/load/207508/.

The Agreement includes an Annex I on the use of terms (referred to in art. 1), as well as an Annex II on threats in cyberspace (referred to in art. 2). Annex I containing the use of terms can be changed and updated as appropriate, allowing more flexibility in the creation of new terms. Annex II on "Basic Types, Sources, and Features of Threats in the Field of International Information Security" can also be updated, as appropriate.

G. Economic Community of West African States (ECOWAS)

In August 2011, ECOWAS adopted a Directive on Fighting Cyber Crime,[60] which prescribes offences specifically related to information and communication technologies, including fraudulent access, interference, data interception, and data modification. The Directive further incorporates traditional offences into information and communication technology offences.[61]

In terms of structure, the Directive first defines key terms within the Directive (Article 1), and explains its objective and scope (articles 2 and 3, respectively). In chapter II, the Directive describes the offences to be criminalized (articles 4 to 23). Chapter III outlines "traditional" offences which are "incorporated into information and communication technology offences" (articles 24 to 27). Chapter IV contains provisions on sanctions (articles 28 to 29). Chapter V contains procedural provisions (articles 30 to Article 33), and chapter VII final provisions.

H. European Union Directive 2013/40/EU on Attacks Against Information Systems

The EU Directive 2013/40/EU of 12 August 2013 on attacks against information systems[62] ('the Directive') is a directive of the European Union seeking to "*approximate the criminal law of* [EU] *Member States in the area of attacks against information systems by establishing minimum rules concerning the definition of criminal offences and the relevant sanctions and to improve cooperation between competent authorities*".[63]

The Directive is applicable to all member States of the European Union, except Denmark, which chose to opt out of its application.[64]

Amongst other provisions, the Directive stresses the importance of common definitions to ensure a consistent approach among member States.[65] In general, the Directive is built on the Budapest Convention on Cybercrime.[66]

As a directive, it is not directly applicable within member States, and needs to be transposed into national law. The limit date for transposition was 4 September 2015 (see article 16, paragraph 1, of the Directive). All member States to which the Directive is applicable appear to have complied with this requirement.[67]

In terms of structure, the Directive delineates in article 1 its subject matter, while containing key definitions in article 2. Articles 3 to 7 prescribe the offences to be criminalized under national law, namely the illegal access to information systems, illegal system and data interference, illegal interception as well as intentionally producing, selling, procuring for use, importing, distributing or otherwise making available specific tools. Articles 8 to 11 contain ancillary provisions, namely on the

[60] Available at https://issafrica.org/ctafrica/uploads/Directive%201:08:11%20on%20Fighting%20Cyber%20Crime%20within%20ECOWAS.pdf.
[61] See information available at https://cyberpolicyportal.org/en/multilateral-frameworks.
[62] English version available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040&from=EN.
[63] Directive, recital 1.
[64] Ibid., recital 32.
[65] Ibid., recital 7.
[66] Ibid., recital 15.
[67] See overview available at https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32013L0040&qid=1634810641057.

incitement, aiding, abetting and attempt, penalties, liability of legal persons, and sanctions against legal persons. Article 12 contains a provision on jurisdiction. Articles 13 to 14 contain provisions on the exchange of information and monitoring and statistics, while articles 14 to 19 contain final provisions.

I. Caribbean Community (CARICOM)

CARICOM has established non-binding Model Legislative Texts of Cybercrime/e-Crimes and Electronic Evidence,[68] which constitute model legislation targeting the prevention and investigation of computer and network related crime. The model offers legal text on preliminary issues, criminal offences, jurisdiction, procedural law, and liability of service providers. The model texts also contain explanatory notes on the meaning of terms used.

J. Commonwealth

The Commonwealth Model Law on Computer and Computer Related Crime [69] provides model provisions on combatting cybercrime in three parts. Part I contains definitions and addresses the jurisdiction of the enacting state.

Part II is concerned with substantive criminal law and the creation of offences. The offences relate to illegal access, interfering with data, interfering with a computer system, the illegal interception of data, illegal devices and child sexual abuse using a computer system or a computer data storage medium. The Model Law does not cover computer-related forgery or fraud. Part III deals with procedural law. It contains provisions on search and seizure warrants, the obligation to assist the police, recording and access to seized data, the production of data, the disclosure of stored traffic data, the preservation of data, the interception of electronic communications and the interception of traffic data, with provisions as to evidence, confidentiality and the limitation of liability together with the necessary definitions.

The Commonwealth Model Law on Electronic Evidence[70] provides a framework for the admissibility and treatment of electronic records in the context of civil, criminal or administrative proceedings in a court or before a tribunal, board or commission.

K. Southern African Development Community (SADC)

The Southern African Development Community Model Laws on Computer Crime and Cybercrime[71] of 2013 are non-binding recommendations by the SADC for national law provisions on computer crime and cybercrime. They have been developed in conformity with the African Union Convention on Cyber Security and Personal Data Protection.[72] They contain model provisions on criminal offences conducted through the use of information and communication technology, jurisdiction, the handling of electronic evidence, procedural law, and liability of service providers.

[68] Section II of document available at https://www.itu.int/en/ITU-D/Cybersecurity/Documents/HIPCAR%20Model%20Law%20Cybercrimes.pdf.
[69] Available at https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/migrated/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf.
[70] Available at https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/migrated/key_reform_pdfs/P15370_7_ROL_Model_Bill_Electronic_Evidence_0.pdf.
[71] Available at https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf.
[72] https://unidir.org/cpp/en/multilateral-frameworks.

III. Content

A. General Provisions

1. Objectives

Article 1 UNTOC. Statement of Purpose

The purpose of this Convention is to promote cooperation to prevent and combat transnational organized crime more effectively.

Article 1 UNCAC. Statement of Purpose

The purposes of this Convention are:

(*a*) To promote and strengthen measures to prevent and combat corruption more efficiently and effectively;

(*b*) To promote, facilitate and support international cooperation and technical assistance in the prevention of and fight against corruption, including in asset recovery;

(*c*) To promote integrity, accountability and proper management of public affairs and public property.

Article 2 Dushanbe Agreement. General Provisions

1. The Parties shall, in accordance with this Agreement, national legislation and international treaties to which they are parties, cooperate to ensure the prevention, detection, suppression, solution and investigation of crimes in the field of information technology.

2. The Parties shall take the necessary organizational and legal measures to implement the provisions of this Agreement.

3. The Parties shall endeavour to converge national legislations in the field of combating information technology crimes.

2. Scope of application

Article 3 UNTOC. Scope of Application

1. This Convention shall apply, except as otherwise stated herein, to the prevention, investigation and prosecution of:

(*a*) The offences established in accordance with articles 5, 6, 8 and 23 of this Convention; and

(*b*) Serious crime as defined in article 2 of this Convention; where the offence is transnational in nature and involves an organized criminal group.

2. For the purpose of paragraph 1 of this article, an offence is transnational in nature if:

(*a*) It is committed in more than one State;

(*b*) It is committed in one State but a substantial part of its preparation, planning, direction or control takes place in another State;

(*c*) It is committed in one State but involves an organized criminal group that engages in criminal activities in more than one State; or

(*d*) It is committed in one State but has substantial effects in another State.

Article 3 UNCAC. Scope of Application

1. This Convention shall apply, in accordance with its terms, to the prevention, investigation and prosecution of corruption and to the freezing, seizure, confiscation and return of the proceeds of offences established in accordance with this Convention.

2. For the purposes of implementing this Convention, it shall not be necessary, except as otherwise stated herein, for the offences set forth in it to result in damage or harm to state property.

3. Protection of sovereignty

Article 4 UNTOC. Protection of Sovereignty

1. States Parties shall carry out their obligations under this Convention in a manner consistent with the principles of sovereign equality and territorial integrity of States and that of non-intervention in the domestic affairs of other States.

2. Nothing in this Convention entitles a State Party to undertake in the territory of another State the exercise of jurisdiction and performance of functions that are reserved exclusively for the authorities of that other State by its domestic law.

Article 4 UNCAC. Protection of Sovereignty

1. States Parties shall carry out their obligations under this Convention in a manner consistent with the principles of sovereign equality and territorial integrity of States and that of non-intervention in the domestic affairs of other States.

2. Nothing in this Convention shall entitle a State Party to undertake in the territory of another State the exercise of jurisdiction and performance of functions that are reserved exclusively for the authorities of that other State by its domestic law.

Article 4 League of Arab States Convention. Safeguarding Sovereignty

1. Every State Party shall commit itself, subject to its own statutes or constitutional principles, to the discharge of its obligations stemming from the application of this convention in a manner consistent with the two principles of equality of the national sovereignty of States and the non-interference in the internal affairs of other States.

2. Nothing in this convention shall allow a State Party to exercise in the territory of another State the jurisdiction or functions the exercising of which is the exclusive right of the authorities of that other State by virtue of its domestic law.

4. Effects of the convention

Article 39 Budapest Convention. Effects of the Convention:

1. The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

- the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);
- the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);
- the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).

2. If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention

other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3. Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 8 SCO Agreement. Relationship with Other International Treaties:

This Agreement shall not interfere with the rights and obligations of each of the Parties under other international treaties they are parties to.

Article 13 Dushanbe Agreement. Relationship to other International Treaties:

This Agreement shall not affect the rights and obligations of each Party deriving for it from other international treaties to which it is a party.

B. Definitions

1. Child/minor

Article 9(3) Budapest Convention. Offences Related to Child Pornography

3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall not be less than 16 years.

2. Child sexual exploitation

Article 1(2) African Union Convention. Definitions

Child pornography means any visual depiction, including any photograph, film, video, image, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

(*a*) the production of such visual depiction involves a minor;

(*b*) such visual depiction is a digital image, computer image, or computer-generated image where a minor is engaging in sexually explicit conduct or when images of their sexual organs are produced or used for primarily sexual purposes and exploited with or without the child's knowledge;

(*c*) such visual depiction has been created, adapted, or modified to appear that a minor is engaging in sexually explicit conduct.

3. Computer data/information (including computer/information program)

Article 1(7) African Union Convention. Definitions

Computerized data means any representation of facts, information or concepts in a form suitable for processing in a computer system;

Article 1(b) Budapest Convention. Definitions

For the purposes of this Convention:

(*b*) "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

Article 2(3-4) League of Arab States Convention. Terminology

For the purposes of this Convention, the following terms shall be defined as follows:

3. *Data*: All that may be stored, processed, generated and transferred by means of information technology, such as numbers, letters, symbols, etc.

4. *Information programme*: A set of instructions or commands which can be executed through means of information technology and are intended to achieve a given task.

Article 1 Dushanbe Agreement. Key Terms

Computer information – information stored in the memory of a computer system, on a computer or other media in a form perceptible to the computer system, or transmitted through communications channels;

4. Computer/information system

Article 1(6) African Union Convention. Definitions

Computer system means an electronic, magnetic, optical, electrochemical, or other high speed data processing device or a group of interconnected or related devices performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or devices;

Art 1(a) Budapest Convention. Definitions

For the purposes of this Convention:

(*a*) "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

Article 2(5) League of Arab States Convention. Terminology

5. *Information system*: A set of programmes and tools intended to process and manage data and information.

Article 1 in combination with Annex 1 SCO Agreement. List of Basic Terms

"Information Infrastructure" means a range of technical tools and systems for formation, generation, transformation, transmission, use and storage of information;

Article 1 Dushanbe Agreement. Key Terms

information system – an organizationally ordered set of tools that implement certain technological actions through information processes designed to solve specific functional tasks;

computer system – a complex of hardware and software designed for automated collection, storage, processing, transmission and receipt of information;

5. Confiscation

Article 2(g) UNCAC

(*g*) "Confiscation", which includes forfeiture where applicable, shall mean the permanent deprivation of property by order of a court or other competent authority;

Article 2(g) UNTOC

(*g*) "Confiscation", which includes forfeiture where applicable, shall mean the permanent deprivation of property by order of a court or other competent authority;

6. Critical infrastructure

Article 1(10) African Union Convention. Definitions

Critical Cyber/ICT Infrastructure means the cyber infrastructure that is essential to vital services for public safety, economic stability, national security, international stability and for the sustainability and restoration of critical cyberspace;

Article 1 in combination with Annex 1 SCO Agreement. List of Basic Terms

"Critically important structures" means facilities, systems and institutions of the state, the impact on which may have consequences directly affecting national security, including the security of an individual, society and the state;

7. Cybercrime/computer crime

Article 1 in combination with Annex 1 SCO Agreement. List of Basic Terms

"Cybercrime" means using information resources and/or influencing them in the information space for illegal purposes;

8. Dual criminality

Article 1(20) African Union Convention. Definitions

Double criminality (dual criminality) means a crime punished in both the country where a suspect is being held and the country asking for the suspect to be handed over or transferred to;

9. Electronic communication/mail

Article 1(21) African Union Convention. Definitions

Electronic communication means any transmission of signs, signals, written material, pictures, sounds or messages of whatsoever nature, to the public or a section of the public by electronic or magnetic means of communication;

Article 1(23) African Union Convention. Definitions

Electronic mail means any message in the form of text, voice, sound or image sent by a public communication network, and stored in a server of the network or in a terminal facility belonging to the addressee until it is retrieved;

10. "Exceeds Authorized Access"

Article 1(28) African Union Convention. Definitions

Exceeds authorized access means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

Article 1 Dushanbe Agreement. Key Terms

unauthorized access to information – access to protected information in violation of rights or rules established by its holder, owner and (or) legislation of the Parties.

11. Indirect electronic communication

Article 1(30) African Union Convention. Definitions

Indirect electronic communication means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient;

12. Information

Article 1(31) African Union Convention. Definitions

Information means any element of knowledge likely to be represented with the aid of devices and to be used, conserved, processed or communicated. Information may be expressed in written, visual, audio, digital and other forms;

13. Information network

Article 2(6) League of Arab States Convention. Terminology

6. *Information Network*: The interconnection between more than one information system to obtain and exchange information.

14. Information technologies

Article 1 Dushanbe Agreement. Key Terms

information technologies – a set of methods, production processes and software and hardware integrated into a technological complex that ensures collection, creation, storage, accumulation, processing, search, output, copying, transfer, distribution and protection of information;

Article 2(5) League of Arab States Convention. Terminology

1. *Information technology*: any material or virtual means or group of interconnected means used to store, sort, arrange, retrieve, process, develop and exchange information according to commands and instructions stored therein. This includes all associated inputs and outputs, by means of wires or wirelessly, in a system or network.

15. (Internet) service provider

Article 1(c) Budapest Convention. Definitions

For the purposes of this Convention:

(*c*) "service provider" means:

(*i*) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

(*ii*) any other entity that processes or stores computer data on behalf of such communication service or users of such service.

Article 2(2) League of Arab States Convention. Terminology

2. *Service provider*: any natural or juridical person, public or private, who provides subscribers with the services needed to communicate through information technology, or who processes or stores information on behalf of the communication service or its users.

16. Malicious program

Article 1 Dushanbe Agreement. Key Terms

malicious program – developed or already existing programs with specially introduced changes knowingly leading to unauthorized destruction, blocking, modification or copying of information, disruption of information (computer) system operation;

17. Proceeds of crime

Article 2(e) UNCAC and UNTOC. Use of Terms

For the purposes of this Convention:

(*e*) "Proceeds of crime" shall mean any property derived from or obtained, directly or indirectly, through the commission of an offence;

18. Property

Article 2(d) UNCAC and UNTOC:

(*d*) "Property" shall mean assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in, such assets;

19. Racism and xenophobia in ICT

Article 1(38) African Union Convention. Definitions

Racism and xenophobia in information and telecommunication technologies means any written material, picture or any other representation of ideas or theories which advocates or encourages or incites hatred, discrimination or violence against any person or group of persons for reasons based on race, colour, ancestry, national or ethnic origin or religion;

20. Seizure of property

Article 2(f) UNCAC and UNTOC

(*f*) "Freezing" or "seizure" shall mean temporarily prohibiting the transfer, conversion, disposition or movement of property or temporarily assuming custody or control of property on the basis of an order issued by a court or other competent authority;

21. Sensitive data

Article 1(41) African Union Convention. Definitions

Sensitive data means all personal data relating to religious, philosophical, political and trade-union opinions and activities, as well as to sex life or race, health, social measures, legal proceedings and penal or administrative sanctions;

22. Subscriber/traffic/content data/information

Article 1(d) Budapest Convention. Definitions

For the purposes of this Convention:

(*d*) "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Article 18(3) Budapest Convention. Production Order

3. For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

(*a*) the type of communication service used, the technical provisions taken thereto and the period of service;

(*b*) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

(*c*) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Article 2(9) League of Arab States Convention. Terminology

9. *Subscriber's information*: Any information that the service provider has concerning the subscribers to the service, except for information through which the following can be known:

(*a*) the type of communication service used, the technical requirements and the period of service.

(*b*) the identity of the subscriber, his postal or geographic address or phone number and the payment information available by virtue of the service agreement or arrangement.

(*c*) any other information on the installation site of the communication equipment by virtue of the service agreement.

C. Criminalization

Paragraph 1 IEG Recommendations

Member States should ensure that their legislative provisions withstand the test of time with regard to future developments in technology by enacting laws with formulations that are technologically neutral and criminalize the activity deemed illegal instead of the means used. Member States, where they deem necessary and appropriate, should also consider establishing consistent terminology to describe cybercrime activities at the domestic level and facilitate, to the extent possible, accurate interpretations of relevant laws by law enforcement agencies and the judiciary.

1. Specialized offences[73]

Paragraph 5 IEG Recommendations

To the extent that they have not done so already, Member States should consider the criminalization of:

(*a*) Illegally gaining access to or hacking into computer systems;

(*b*) Illegally intercepting or damaging computer data and damaging computer systems;

(*c*) Illegally interfering with computer data and systems.

(a) Illegal access

Article 29(1)(a)(b) African Union Convention. Offences Specific to Information and Communication Technologies

1. Attacks on computer systems

State Parties shall take the necessary legislative and/or regulatory measures to make it a criminal offence to:

1. Gain or attempt to gain unauthorized access to part or all of a computer system or exceed authorized access;

2. Gain or attempt to gain unauthorized access to part or all of a computer system or exceed authorized access with intent to commit another offence or facilitate the commission of such an offence;

Article 2 Budapest Convention. Illegal Access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally,

[73] Cf. Cybercrime Study 2013, p. 51

the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 6 League of Arab States Convention. Offense of Illicit Access

1. Illicit access to, presence in or contact with part or all of information technology, or the perpetuation thereof.

2. The punishment shall be increased if this access, presence, contact or perpetuation leads to:

(*a*) the obliteration, modification, distortion, duplication, removal or destruction of saved data, electronic instruments and systems and communication networks, and damages to the users and beneficiaries.

(*b*) the acquirement of secret government information.

(b) Illegal interception or acquisition of data

Article 3 Budapest Convention. Illegal Interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 7 League of Arab States Convention. Offense of Illicit Interception

The deliberate unlawful interception of the movement of data by any technical means, and the disruption of transmission or reception of information technology data.

Article 29(2)(a) African Union Convention. Offences Specific to Information and Communication Technologies

2. Computerized Data Breaches

State Parties shall take the necessary legislative and/or regulatory measures to make it a criminal offence to:

1. Intercept or attempt to intercept computerized data fraudulently by technical means during non-public transmission to, from or within a computer system;

(c) Illegal interference

Article 4 Budapest Convention. Data Interference

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 Budapest Convention. System Interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 League of Arab States Convention. Offense of Illicit Access

1. Illicit access to, presence in or contact with part or all of information technology, or the perpetuation thereof.

2. The punishment shall be increased if this access, presence, contact or perpetuation leads to:

(*a*) the obliteration, modification, distortion, duplication, removal or destruction of saved data, electronic instruments and systems and communication networks, and damages to the users and beneficiaries.

(*b*) the acquirement of secret government information.

Article 8 League of Arab States Convention. Offence Against the Integrity of Data

1. Deliberate unlawful destruction, obliteration, obstruction, modification or concealment of information technology data.

2. The Party may require that, in order to criminalize acts mentioned in paragraph 1, they must cause severe damage.

Article 29(1)(e)(f) African Union Convention. Offences Specific to Information and Communication Technologies

1. Attacks on Computer Systems

State Parties shall take the necessary legislative and/or regulatory measures to make it a criminal offence to: …

(*e*) Enter or attempt to enter data fraudulently in a computer system;

(*f*) Damage or attempt to damage, delete or attempt to delete, deteriorate or attempt to deteriorate, alter or attempt to alter, change or attempt to change computer data fraudulently.

Article 3(1)(a)(c) Dushanbe Agreement. Punishable Acts

1. The Parties shall criminalize, in accordance with national law, the following acts in the field of information technologies, when committed intentionally:

(*a*) destruction, blocking, modification or copying of information, disruption of the operation of information (computer) system through unauthorized access to legally protected computer information;

(*c*) violation of operating rules of a computer system by a person who has access to it, resulting in destruction, blocking or modification of legally protected computer information, if the act has caused significant harm or serious consequences;

(d) Misuse of devices/information technology means

Article 6 Budapest Convention. Misuse of Devices

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

(*a*) the production, sale, procurement for use, import, distribution or otherwise making available of:

(*i*) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

(*ii*) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

(*b*) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Article 9 League of Arab States Convention. Offence of Misuse of Information Technology Means

1. The production, sale, purchase, import, distribution or provision of:

(*a*) any tools or programmes designed or adapted for the purpose of committing the offences indicated in Articles 6 to 8.

(*b*) the information system password, access code or similar information that allows access to the information system with the aim of using it for any of the offences indicated in Articles 6 to 8.

2. The acquisition of any tools or programmes mentioned in the two paragraphs above with the aim of using them to commit any of the offences indicated in Articles 6 to 8.

Article 3(1)(b)(f), Dushanbe Agreement. Punishable Acts

1. The Parties shall criminalize, in accordance with national law, the following acts in the field of information technologies, when committed intentionally:

(*b*) the creation, use or distribution of malicious programs;

(*f*) the manufacture for sale or sale of special software or hardware for obtaining unauthorized access to a protected computer system or network;

2. Offences for criminal acts which are enabled through the use of ICTs

Paragraph 4 IEG Recommendations

Member States should take into account that many substantive criminal law provisions designed for “offline” crime may also be applicable to crimes committed online. Therefore, to strengthen law enforcement, Member States should use existing provisions in domestic and international law, as appropriate, to tackle crimes in the online environment.

(a) Forgery

Article 7 Budapest Convention. Computer-Related Forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 10 League of Arab States Convention. Offence of Forgery

The use of information technology means to alter the truth of data in a manner that causes harm, with the intent of using them as true data.

Article 18 League of Arab States Convention. Illicit Use of Electronic Payment Tools

1. Any person who forges, manufactures or sets up any instrument or materials that assist in the forgery or imitation of any electronic payment tool by whatever means.

2. Any person who takes possession of the data of an electronic payment tool and uses it, gives it to a third party or facilitates its acquisition by a third party.

3. Any person who uses the information network or an information technology means to unlawfully access the numbers or data of a payment tool.

4. Any person who knowingly accept a forged payment tool.

(b) Fraud

Article 8 Budapest Convention. Computer-Related Fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

(*a*) any input, alteration, deletion or suppression of computer data,

(*b*) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Article 11 League of Arab States Convention. Offence of Fraud

Intentionally and unlawfully causing harm to beneficiaries and users with the aim of committing fraud to illicitly realize interests and benefits to the perpetrator or a third party, through:

1. entering, modifying, obliterating or concealing information and data.

2. interfering with the functioning of the operation systems and communication systems, or attempting to disrupt or change them.

3. disrupting electronic instruments, programmes and sites.

Article 29(2)(d) African Union Convention. Offences Specific to Information and Communication Technologies. Computerized Data Breaches

State Parties shall take necessary legislative and/or regulatory measures to make it a criminal offence to:

(*d*) Fraudulently procure, for oneself or for another person, any benefit by inputting, altering, deleting or suppressing computerized data or any other form of interference with the functioning of a computer system;

Article 30(1)(a)(b) African Union Convention. Adapting Certain Offences to Information and Communication Technologies

1. Property Offences

(*a*) State Parties shall take the necessary legislative and/or regulatory measures to criminalize the violation of property such as theft, fraud, handling of stolen property, abuse of trust, extortion of funds and blackmail involving computer data;

(*b*) State Parties shall take the necessary legislative and/or regulatory measures to consider as aggravating circumstances the use of information and

communication technologies to commit offences such as theft, fraud, handling of stolen property, abuse of trust, extortion of funds, terrorism and money laundering;

(c) Theft

Article 3(1)(d) Dushanbe Agreement. Punishable Acts

1. The Parties shall criminalize, in accordance with national law, the following acts in the field of information technologies, when committed intentionally: (*d*) theft of property by modifying information processed in a computer system, stored on computer media or transmitted via data transmission networks, or by entering into a computer system false information, or involving unauthorized access to legally protected computer information;

(d) Electronic payment tools offences

Article 18 League of Arab States Convention. Illicit Use of Electronic Payment Tools

1. Any person who forges, manufactures or sets up any instrument or materials that assist in the forgery or imitation of any electronic payment tool by whatever means.

2. Any person who takes possession of the data of an electronic payment tool and uses it, gives it to a third party or facilitates its acquisition by a third party.

3. Any person who uses the information network or an information technology means to unlawfully access the numbers or data of a payment tool.

4. Any person who knowingly accept a forged payment tool.

(e) Copyright and trademark offences

Article 10 Budapest Convention. Offences Related to Infringements of Copyright and Related Rights

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Article 17 League of Arab States Convention. Offenses Related to Copyright and Adjacent Rights

Violation of copyright as defined according to the law of the State Party, if the act is committed deliberately and for no personal use, and violation of rights adjacent to the

relevant copyright as defined according to the law of the State Party, if the act is committed deliberately and for no personal use.

Article 3(1)(g), Dushanbe Agreement. Punishable Acts

1. The Parties shall criminalize, in accordance with national law, the following acts in the field of information technologies, when committed intentionally:

(*g*) unlawful use of programs for computer systems and databases, which are objects of copyright, as well as usurpation of authorship, if this act has caused substantial damage;

(f) Acts involving racism or xenophobia

Article 3 First Additional Protocol to the Budapest Convention. Dissemination of Racist and Xenophobic Material Through Computer Systems

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

distributing, or otherwise making available, racist and xenophobic material to the public through a computer system.

2. A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available.

3. Notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2.

Article 4 First Additional Protocol to the Budapest Convention. Racist and Xenophobic Motivated Threat

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.

Article 5 First Additional Protocol to the Budapest Convention. Racist and Xenophobic Motivated Insult

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics.

2. A Party may either:

(*a*) require that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule; or

(*b*) reserve the right not to apply, in whole or in part, paragraph 1 of this article.

Article 29(3)(e)(f)(g), AU Convention 2014. Offences Specific to Information and Communication Technologies. Content Related Offences

State Parties shall take the necessary legislative and/or regulatory measures to make it a criminal offence to:

(*e*) Create, download, disseminate or make available in any form writings, messages, photographs, drawings or any other presentation of ideas or theories of racist or xenophobic nature through a computer system;

(*f*) Threaten, through a computer system, to commit a criminal offence against a person for the reason that they belong to a group distinguished by race, colour, descent, national or ethnic origin or religion where such membership serves as a pretext for any of these factors, or against a group of persons which is distinguished by any of these characteristics;

(*g*) Insult, through a computer system, persons for the reason that they belong to a group distinguished by race, colour, descent, national or ethnic origin, or religion or political opinion, if used as a pretext for any of these factors, or against a group of persons distinguished by any of these characteristics;

(g) Denial or justification of genocide or crimes against humanity

Article 6 First Additional Protocol to the Budapest Convention. Denial, Gross Minimisation, Approval or Justification of Genocide or Crimes against Humanity

1. Each Party shall adopt such legislative measures as may be necessary to establish the following conduct as criminal offences under its domestic law, when committed intentionally and without right:

distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognised by that Party.

2. A Party may either

(*a*) require that the denial or the gross minimisation referred to in paragraph 1 of this article is committed with the intent to incite hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or otherwise

(*b*) reserve the right not to apply, in whole or in part, paragraph 1 of this article.

Article 29(3)(h) AU Convention 2014. Offences Specific to Information and Communication Technologies. Content Related Offences

State Parties shall take the necessary legislative and/or regulatory measures to make it a criminal offence to:

(*h*) Deliberately deny, approve or justify acts constituting genocide or crimes against humanity through a computer system.

(h) Computer-related production, possession, or distribution of child pornography/sexual abuse

Paragraph 56 IEG Recommendations

Countries should consider specific and tailored efforts to keep children safe online. This should include ensuring domestic legal frameworks, practical arrangements and international cooperation arrangements to enable reporting, detection, investigation, prosecution and deterrence of child sexual abuse and exploitation online.

Article 9 Budapest Convention. Offences Related to Child Pornography

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

(*a*) producing child pornography for the purpose of its distribution through a computer system;

(*b*) offering or making available child pornography through a computer system;

(*c*) distributing or transmitting child pornography through a computer system;

(*d*) procuring child pornography through a computer system for oneself or for another person;

(*e*) possessing child pornography in a computer system or on a computer-data storage medium.

2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

(*a*) a minor engaged in sexually explicit conduct;

(*b*) a person appearing to be a minor engaged in sexually explicit conduct;

(*c*) realistic images representing a minor engaged in sexually explicit conduct.

3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, subparagraphs d and e, and 2, sub-paragraphs b and c.

Article 12 League of Arab States Convention. Offence of Pornography

1. The production, display, distribution, provision, publication, purchase, sale, import of pornographic material or material that constitutes outrage of modesty through information technology.

2. The punishment shall be increased for offences related to children and minors pornography.

3. The increase mentioned in paragraph 2 of this Article covers the acquisition of children and minors pornographic material or children and minors material that constitutes outrage of modesty, through information technology or a storage medium for such technology.

Article 29(3)(1)(a-d) African Union Convention. Offences Specific to Information and Communication Technologies. Content Related Offences

1. State Parties shall take the necessary legislative and/or regulatory measures to make it a criminal offence to:

(*a*) Produce, register, offer, manufacture, make available, disseminate and transmit an image or a representation of child pornography through a computer system;

(*b*) Procure for oneself or for another person, import or have imported, and export or have exported an image or representation of child pornography through a computer system;

(*c*) Possess an image or representation of child pornography in a computer system or on a computer data storage medium;

(*d*) Facilitate or provide access to images, documents, sound or representation of a pornographic nature to a minor;

Article 3(1)(e) Dushanbe Agreement. Punishable Acts

1. The Parties shall criminalize, in accordance with national law, the following acts in the field of information technologies, when committed intentionally:

(*e*) dissemination of pornographic materials or items of pornographic nature depicting a minor through the Internet or other electrical communication channels;

(i) Acts in support of extremism/terrorism

Article 15 League of Arab States Convention. Offences Related to Terrorism Committed by Means of Information technology

1. Dissemination and advocacy of the ideas and principles of terrorist groups.

2. Financing of and training for terrorist operations, and facilitating communication between terrorist organizations.

3. Dissemination of methods to make explosives, especially for use in terrorist operations.

4. Spreading religious fanaticism and dissention and attacking religions and beliefs.

Article 3(1)(h) Dushanbe Agreement. Punishable Acts

1. The Parties shall criminalize, in accordance with national law, the following acts in the field of information technologies, when committed intentionally:

(*h*) the dissemination with the use of the Internet or other electrical communication channels of materials recognized in accordance with the established procedure as extremist or containing calls for terrorist activities or justification of terrorism.

(j) Offences related to organized crime committed by means of information technology

Article 16 League of Arab States Convention. Offences Related to Organized Crime Committed by Means of Information Technology

1. Undertake money-laundering operations, request assistance or disseminate money-laundering methods.

2. Advocate the use of and traffic in drugs and Psychotropic Substances.

3. Traffic in persons.

4. Traffic in human organs

5. Illicit traffic in arms.

(k) Offences against morality and privacy

Article 12 League of Arab States Convention. Offence of Pornography

1. The production, display, distribution, provision, publication, purchase, sale, import of pornographic material or material that constitutes outrage of modesty through information technology.

2. The punishment shall be increased for offences related to children and minors pornography.

3. The increase mentioned in paragraph 2 of this Article covers the acquisition of children and minors pornographic material or children and minors material that constitutes outrage of modesty, through information technology or a storage medium for such technology.

Article 13 League of Arab States Convention. Other Offences Related to Pornography

Gambling and sexual exploitation.

Article 14 League of Arab States Convention. Offence Against Privacy

Offence against privacy by means of information technology.

3. Ancillary provisions for criminalization

(a) Aggravating circumstances for conventional crime committed by means of information and communications technology

Article 21 League of Arab States Convention. Increasing Punishment for Traditional Crimes Committed by Means of Information Technology

Every State Party shall commit itself to increasing the punishment for traditional crimes when they are committed by means of information technology.

Article 30(1)(b), AU Convention 2014. Adapting Certain Offences to Information and Communication Technologies. Property Offences

State Parties shall take the necessary legislative and/or regulatory measures to consider as aggravating circumstances the use of information and communication technologies to commit offences such as theft, fraud, handling of stolen property, abuse of trust, extortion of funds, terrorism and money laundering;

(b) More severe sanctions for attacks against critical infrastructure

Article 25 para. 4 AU Convention 2014. Legal Measures. Protection of Critical Infrastructure

Each State Party shall adopt such legislative and/or regulatory measures as they deem necessary to identify the sectors regarded as sensitive for their national security and well-being of the economy, as well as the information and communication technologies systems designed to function in these sectors as elements of critical information infrastructure; and, in this regard, proposing more severe sanctions for criminal activities on ICT systems in these sectors, as well as measures to improve vigilance, security and management.

(c) Participation, attempt, aiding, abetting

Article 27 UNCAC. Participation and Attempt

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence, in accordance with its domestic law, participation in any capacity such as an accomplice, assistant or instigator in an offence established in accordance with this Convention.

2. Each State Party may adopt such legislative and other measures as may be necessary to establish as a criminal offence, in accordance with its domestic law, any attempt to commit an offence established in accordance with this Convention.

3. Each State Party may adopt such legislative and other measures as may be necessary to establish as a criminal offence, in accordance with its domestic law, the preparation for an offence established in accordance with this Convention.

Article 11 Budapest Convention. Attempt and Aiding or Abetting

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c of this Convention.

3. Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 7 First Additional Protocol to the Budapest Convention. Aiding and Abetting

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, aiding or abetting the commission of any of the offences established in accordance with this Protocol, with intent that such offence be committed.

Article 29(2)(f), AU Convention 2014. Offences Specific to Information and Communication Technologies. Computerized Data Breaches

State Parties shall take the necessary legislative and/or regulatory measures to make it a criminal offence to:

(*f*) Participate in an association formed or in an agreement established with a view to preparing or committing one or several of the offences provided for under this Convention.

(d) Liability of legal persons

Article 10 UNTOC. Liability of Legal Persons

1. Each State Party shall adopt such measures as may be necessary, consistent with its legal principles, to establish the liability of legal persons for participation in serious crimes involving an organized criminal group and for the offences established in accordance with articles 5, 6, 8 and 23 of this Convention.

2. Subject to the legal principles of the State Party, the liability of legal persons may be criminal, civil or administrative.

3. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offences.

4. Each State Party shall, in particular, ensure that legal persons held liable in accordance with this article are subject to effective, proportionate and dissuasive criminal or non-criminal sanctions, including monetary sanctions.

Article 26 UNCAC. Liability of Legal Persons

1. Each State Party shall adopt such measures as may be necessary, consistent with its legal principles, to establish the liability of legal persons for participation in the offences established in accordance with this Convention.

2. Subject to the legal principles of the State Party, the liability of legal persons may be criminal, civil or administrative.

3. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offences.

4. Each State Party shall, in particular, ensure that legal persons held liable in accordance with this article are subject to effective, proportionate and dissuasive criminal or non-criminal sanctions, including monetary sanctions.

Article 12 Budapest Convention. Corporate Liability

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

(*a*) a power of representation of the legal person;

(*b*) an authority to take decisions on behalf of the legal person;

(*c*) an authority to exercise control within the legal person.

2. In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 30(2) AU Convention 2014. Adapting Certain Offences to Information and Communication Technologies. Criminal Liability for Legal Persons

State Parties shall take the necessary legislative measures to ensure that legal persons other than the State, local communities and public institutions can be held responsible for the offences provided for by this Convention, committed on their behalf by their organs or representatives. The liability of legal persons does not exclude that of the natural persons who are the perpetrators of or accomplices in the same offences.

(e) Knowledge, intent and purpose as elements of an offence

Article 28 UNCAC. Knowledge, Intent and Purpose as Elements of an Offence

Knowledge, intent or purpose required as an element of an offence established in accordance with this Convention may be inferred from objective factual circumstances.

(f) Statute of limitations

Article 29 UNCAC. Statute of Limitations

Each State party shall, where appropriate, establish under its domestic law a long statute of limitations period in which to commence proceedings for any offence established in accordance with this Convention and establish a longer statute of limitations period or provide for the suspension of the statute of limitations where the alleged offender has evaded the administration of justice.

(g) Prosecution, adjudication and sanctions

Article 11 UNTOC. Prosecution, Adjudication and Sanctions

1. Each State Party shall make the commission of an offence established in accordance with articles 5, 6, 8 and 23 of this Convention liable to sanctions that take into account the gravity of that offence.

2. Each State Party shall endeavour to ensure that any discretionary legal powers under its domestic law relating to the prosecution of persons for offences covered by this Convention are exercised to maximize the effectiveness of law enforcement measures in respect of those offences and with due regard to the need to deter the commission of such offences.

3. In the case of offences established in accordance with articles 5, 6, 8 and 23 of this Convention, each State Party shall take appropriate measures, in accordance with its domestic law and with due regard to the rights of the defence, to seek to ensure that conditions imposed in connection with decisions on release pending trial or appeal take into consideration the need to ensure the presence of the defendant at subsequent criminal proceedings.

4. Each State Party shall ensure that its courts or other competent authorities bear in mind the grave nature of the offences covered by this Convention when considering the eventuality of early release or parole of persons convicted of such offences.

5. Each State Party shall, where appropriate, establish under its domestic law a long statute of limitations period in which to commence proceedings for any offence covered by this Convention and a longer period where the alleged offender has evaded the administration of justice.

6. Nothing contained in this Convention shall affect the principle that the description of the offences established in accordance with this Convention and of the applicable legal defences or other legal principles controlling the lawfulness of conduct is reserved to the domestic law of a State Party and that such offences shall be prosecuted and punished in accordance with that law.

Article 30 UNCAC. Prosecution, Adjudication and Sanctions

1. Each State Party shall make the commission of an offence established in accordance with this Convention liable to sanctions that take into account the gravity of that offence.

2. Each State Party shall take such measures as may be necessary to establish or maintain, in accordance with its legal system and constitutional principles, an appropriate balance between any immunities or jurisdictional privileges accorded to its public officials for the performance of their functions and the possibility, when necessary, of effectively investigating, prosecuting and adjudicating offences established in accordance with this Convention.

3. Each State Party shall endeavour to ensure that any discretionary legal powers under its domestic law relating to the prosecution of persons for offences established in accordance with this Convention are exercised to maximize the effectiveness of law enforcement measures in respect of those offences and with due regard to the need to deter the commission of such offences.

4. In the case of offences established in accordance with this Convention, each State Party shall take appropriate measures, in accordance with its domestic law and with due regard to the rights of the defence, to seek to ensure that conditions imposed in connection with decisions on release pending trial or appeal take into consideration the need to ensure the presence of the defendant at subsequent criminal proceedings.

5. Each State Party shall take into account the gravity of the offences concerned when considering the eventuality of early release or parole of persons convicted of such offences.

6. Each State Party, to the extent consistent with the fundamental principles of its legal system, shall consider establishing procedures through which a public official accused of an offence established in accordance with this Convention may, where appropriate, be removed, suspended or reassigned by the appropriate authority, bearing in mind respect for the principle of the presumption of innocence.

7. Where warranted by the gravity of the offence, each State Party, to the extent consistent with the fundamental principles of its legal system, shall consider establishing procedures for the disqualification, by court order or any other appropriate means, for a period of time determined by its domestic law, of persons convicted of offences established in accordance with this Convention from:

(*a*) Holding public office; and

(*b*) Holding office in an enterprise owned in whole or in part by the State.

8. Paragraph 1 of this article shall be without prejudice to the exercise of disciplinary powers by the competent authorities against civil servants.

9. Nothing contained in this Convention shall affect the principle that the description of the offences established in accordance with this Convention and of the applicable legal defences or other legal principles controlling the lawfulness of conduct is reserved to the domestic law of a State Party and that such offences shall be prosecuted and punished in accordance with that law.

10. States Parties shall endeavour to promote the reintegration into society of persons convicted of offences established in accordance with this Convention.

Article 13 Budapest Convention. Sanctions and Measures

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2. Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Article 31(1)(2) AU Convention 2014. Adapting Certain Sanctions to Information and Communication Technologies

1. Criminal sanctions

(*a*) State parties shall take the necessary legislative measures to ensure that the offences provided for under this Convention are punishable by effective, proportionate and dissuasive criminal penalties;

(*b*) State Parties shall take the necessary legislative measures to ensure that the offences provided for under this Convention are punishable by appropriate penalties under their national legislations;

(*c*) State Parties shall take the necessary legislative measures to ensure that a legal person held liable pursuant to the terms of this Convention is punishable by effective, proportionate and dissuasive sanctions, including criminal fines.

2. Other criminal sanctions

(*a*) State Parties shall take the necessary legislative measures to ensure that in the case of conviction for an offense committed through a digital communication medium, the competent court may hand down additional sanctions;

(*b*) State Parties shall take the necessary legislative measures to ensure that in the case of conviction for an offence committed through a digital communication medium, the judge may in addition order the mandatory dissemination, at the expense of the convicted person, of an extract of the decision, through the same medium, and according to modalities prescribed by the law of Member States;

(*c*) State Parties shall take the necessary legislative measures to ensure that a breach of the confidentiality of data stored in a computer system is punishable by the same penalties as those applicable for breached of professional secrecy.

(h) Consideration of criminal record in another state

Article 41 UNCAC. Criminal Record

Each State Party may adopt such legislative or other measures as may be necessary to take into consideration, under such terms as and for the purpose that it deems appropriate, any previous conviction in another State of an alleged offender for the purpose of using such information in criminal proceedings relating to an offence established in accordance with this Convention.

Article 22 UNTOC. Establishment of Criminal Record

Each State Party may adopt such legislative or other measures as may be necessary to take into consideration, under such terms as and for the purpose that it deems appropriate, any previous conviction in another State of an alleged offender for the purpose of using such information in criminal proceedings related to an offence covered by this Convention.

D. Jurisdiction

1. Territorial principle

Article 15(1)(a)(b) UNTOC

1. Each State Party shall adopt such measures as may be necessary to establish its jurisdiction over the offences established in accordance with article 5, 6, 8 and 23 of this Convention when:

(*a*) The offence is committed in the territory of that State Party;

(*b*) The offence is committed on board a vessel that is flying the flag of that State Party or an aircraft that is registered under the laws of that State Party at the time that the offence is committed.

Article 42(1)(a)(b) UNCAC. Jurisdiction

1. Each State Party shall adopt such measures as may be necessary to establish its jurisdiction over the offences established in accordance with this Convention when:

(*a*) The offence is committed in the territory of that State Party; or

(*b*) The offence is committed on board a vessel that is flying the flag of that State Party or an aircraft that is registered under the laws of that State Party at the time that the offence is committed.

Article 22(1)(a-c) Budapest Convention. Jurisdiction

1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

(*a*) in its territory;

(*b*) on board a ship flying the flag of that Party; or

(*c*) on board an aircraft registered under the laws of that Party;

Article 30(1)(a), League of Arab States Convention. Competence

1. Every State Party shall commit itself to adopting the procedures necessary to extend its competence to any of the offences set forth in Chapter II of this Convention, if the offence is committed, partly or totally, or was realized:

(*a*) in the territory of the State Party

(*b*) on board a ship raising the flag of the State Party.

(*c*) on board a plane registered under the law of the State Party.

2. Nationality principle (offender/active)

Article 15(2)(b), UNTOC. Jurisdiction

2. Subject to article 4 of this Convention, a State Party may also establish its jurisdiction over any such offence when:

(*b*) The offence is committed by a national of that State Party or a stateless person who has his or her habitual residence in its territory;

Article 42(2)(b) UNCAC. Jurisdiction

2. Subject to article 4 of this Convention, a State Party may also establish its jurisdiction over any such offence when:

(*b*) The offence is committed by a national of that State Party or a stateless person who has his or her habitual residence in its territory;

Article 22(1)(d) Budapest Convention. Jurisdiction

1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: …

(*d*) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

Article 30(1)(d) League of Arab States Convention. Competence

1. Every State Party shall commit itself to adopting the procedures necessary to extend its competence to any of the offences set forth in Chapter II of this Convention, if the offence is committed, partly or totally, or was realized:

(*d*) by a national of the State Party if the offence is punishable according to the domestic law in the location where it was committed, or if it was committed outside the jurisdiction of any State.

3. Nationality principle (victim/passive)

Article 15(2)(a) UNTOC. Jurisdiction

2. Subject to article 4 of this Convention, a State Party may also establish its jurisdiction over any such offence when:

(*a*) The offence is committed against a national of that State Party;

Article 42(2)(a) UNCAC. Jurisdiction

2. Subject to article 4 of this Convention, a State Party may also establish its jurisdiction over any such offence when:

(*a*) The offence is committed against a national of that State Party;

4. State interests principle

Article 42(2)(d) UNCAC. Jurisdiction

2. Subject to article 4 of this Convention, a State Party may also establish its jurisdiction over any such offence when:

(*d*) The offence is committed against the State Party.

Article 30(1)(e) League of Arab States Convention. Competence

1. Every State Party shall commit itself to adopting the procedures necessary to extend its competence to any of the offences set forth in Chapter II of this Convention, if the offence is committed, partly or totally, or was realized:

(*e*) if the offence affects an overriding interest of the State.

5. Jurisdiction when extradition is refused

Article 15(3)(4) UNTOC. Jurisdiction

3. For the purposes of article 16, paragraph 10, of this Convention, each State Party shall adopt such measures as may be necessary to establish its jurisdiction over the offences covered by this Convention when the alleged offender is present in its territory and it does not extradite such person solely on the ground that he or she is one of its nationals.

4. Each State Party may also adopt such measures as may be necessary to establish its jurisdiction over the offences covered by this Convention when the alleged offender is present in its territory and it does not extradite him or her.

Article 42(3)(4) UNCAC. Jurisdiction

3. For the purposes of article 44 of this Convention, each State Party shall take such measures as may be necessary to establish its jurisdiction over the offences established in accordance with this Convention when the alleged offender is present in its territory and it does not extradite such person solely on the ground that he or she is one of its nationals.

4. Each State Party may also take such measures as may be necessary to establish its jurisdiction over the offences established in accordance with this Convention when the alleged offender is present in its territory and it does not extradite him or her.

Article 22(3) Budapest Convention. Jurisdiction

3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

Article 30(2) League of Arab States Convention. Competence

2. Every State Party shall commit itself to adopting the procedures necessary to extend the competence covering the offences set forth in Article 31, paragraph 1, of this Convention in the cases in which the alleged offender is present in the territory of that State Party and shall not extradite him to another Party according to his nationality following the extradition request.

6. Conflict of jurisdictions

Article 15(5) UNTOC. Jurisdiction

5. If a State Party exercising its jurisdiction under paragraph 1 or 2 of this article has been notified, or has otherwise learned, that one or more other States Parties are conducting an investigation, prosecution or judicial proceeding in respect of the same conduct, the competent authorities of those States Parties shall, as appropriate, consult one another with a view to coordinating their actions.

Article 42(5) UNCAC. Jurisdiction

5. If a State Party exercising its jurisdiction under paragraph 1 or 2 of this article has been notified, or has otherwise learned, that any other States Parties are conducting an investigation, prosecution or judicial proceeding in respect of the same conduct, the competent authorities of those States Parties shall, as appropriate, consult one another with a view to coordinating their actions.

Article 22(5) Budapest Convention. Jurisdiction

When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Article 30(3) League of Arab States Convention. Competence

3. If more than one State Party claim to have jurisdiction over an offence set forth in this Convention, priority shall be accorded to the request of the State whose security or interests were disrupted by the offence, followed by the State in whose territory the offence was committed, and then by the State of which the wanted person is a national. In case of similar circumstances, priority shall be accorded to the first State that requests the extradition.

E. Procedural Powers

Paragraph 10 IEG Recommendations

Domestic procedural laws must keep pace with technological advances and ensure that law enforcement authorities are adequately equipped to combat cybercrime. Relevant laws should be drafted taking into account applicable technical concepts and the practical needs of cybercrime investigators, consistent with due process, privacy, human rights and fundamental freedoms. Moreover, Member States should devote resources to enacting domestic legislation that authorizes:

(*a*) The real-time collection of traffic data and content in appropriate cases;

(*b*) International cooperation by domestic law enforcement authorities.

Paragraph 17 IEG Recommendations

Member States should develop and implement legal frameworks, jurisdictional rules and other procedural provisions to ensure that cybercrime can be effectively investigated at the national level and that effective international cooperation can be

achieved in that regard through effective law enforcement, with respect for national sovereignty, and the protection of privacy and all human rights. This may include:

(*a*) The adjustment of rules of evidence to ensure that electronic evidence can be collected, preserved, authenticated and used in criminal proceedings;

(*b*) The adoption of provisions on the national and international tracing of communications.

1. Scope of procedural provisions

Article 14 Budapest Convention. Scope of Procedural Provisions

1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2. Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

(*a*) the criminal offences established in accordance with Articles 2 through 11 of this Convention;

(*b*) other criminal offences committed by means of a computer system; and

(*c*) the collection of evidence in electronic form of a criminal offence.

3. (*a*) Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

(*b*) Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

(*i*) is being operated for the benefit of a closed group of users, and

(*ii*) does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 31(3) AU Convention 2014. Adapting Certain Sanctions to Information and Communication Technologies

3. Procedural law

(*a*) State Parties shall take the necessary legislative measures to ensure that where the data stored in a computer system or in medium where computerized data can be stored in the territory of a State Party, are useful in establishing the truth, the court applied to may carry out a search to access all or part of a computer system through another computer system, where the said data are accessible from or available to the initial system;

(*b*) State Parties shall take the necessary legislative measures to ensure that where the judicial authority in charge of investigation discovers data stored in a computer system that are useful for establishing the truth, but the seizure of the support does not seem to be appropriate, the data as well as all such data as are required to understand them, shall be copied into a computer storage medium that can be seized and sealed, in accordance with the modalities provided for under the legislations of State Parties;

(*c*) State Parties shall take the necessary legislative measures to ensure that judicial authorities can, for the purposes of investigation or execution of a judicial delegation, carry out the operations provided for under this Convention;

(*d*) State Parties shall take the necessary legislative measures to ensure that if information needs so require, particularly where there are reasons to believe that the information stored in a computer system are particularly likely to be lost or modified, the investigating judge may impose an injunction on any person to preserve and protect the integrity of the data in his/her possession or under his/her control, for a maximum period of two years, in order to ensure the smooth conduct of the investigation. The custodian of the data or any other person responsible for preserving the data shall be expected to maintain secrecy with regard to the data;

(*e*) State Parties shall take the necessary legislative measures to ensure that where information needs so require, the investigating judge can use appropriate technical means to collect or record in real time, data in respect of the contents of specific communications in its territory, transmitted by means of a computer system or compel a service provider, within the framework of his/her technical capacities, to collect and record, using the existing technical facilities in its territory or that of State Parties, or provide support and assistance to the competent authorities towards the collection and recording of the said computerized data.

2. Expedited preservation of stored computer data/data stored in information technology

Article 16 Budapest Convention. Expedited Preservation of Stored Computer Data

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 23 League of Arab States Convention. Expeditious Custody of Data Stored in Information Technology

1. Every State Party shall adopt the procedures necessary to enable the competent authorities to issue orders or obtain the expeditious custody of information, including information for tracking users, that was stored on an information technology, especially if it is believed that such information could be lost or amended.

2. Every State Party shall commit itself to adopting the procedures necessary as regards paragraph 1, by means of issuing an order to a person to preserve the information technology information in his possession or under his control, in order to require him to preserve and maintain the integrity of such information for a maximum period of 90 days that may be renewed, in order to allow the competent authorities to search and investigate.

3. Every State Party shall commit itself to adopting the procedures necessary to require the person responsible for safeguarding the information technology to maintain the procedures secrecy throughout the legal period stated in the domestic law.

3. Expedited preservation and partial disclosure of traffic data

Article 17 Budapest Convention. Expedited Preservation and Partial Disclosure of Traffic Data

1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

(*a*) ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

(*b*) ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 24, League of Arab States Convention. Expeditious Custody and Partial Disclosure of Users Tracking Information

Every State Party shall commit itself to adopting the procedures necessary as regards users tracking information in order to:

1. ensure expeditious custody of users tracking information, regardless of whether such communication is transmitted by one or more service providers.

2. ensure that a sufficient amount of users tracking information is disclosed to the competent authorities of the State Party or to a person appointed by these authorities to allow the State Party to determine the service providers and the transmission path of the communications.

4. Order to submit information stored in an electronic medium

Article 25(1) League of Arab States Convention. Order to Submit Information

Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to issue orders to:

1. Any person in its territory to submit certain information in his possession which is stored on information technology or a medium for storing information.

5. Order for subscriber information

Article 18(1)(b) Budapest Convention. Production Order

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

(*b*) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

Article 25(2) League of Arab States Convention. Order to Submit Information

Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to issue orders to:

2. Any service provider offering his services in the territory of the State Party to submit user's information related to that service which is in the possession of the service provider or under his control.

6. Order for stored traffic data

Article 17(1)(b) Budapest Convention. Expedited Preservation and Partial Disclosure of Traffic Data

1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

(*b*) ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

Article 24 League of Arab States Convention. Expeditious Custody and Partial Disclosure of Users Tracking Information

Every State Party shall commit itself to adopting the procedures necessary as regards users tracking information in order to:

1. ensure expeditious custody of users tracking information, regardless of whether such communication is transmitted by one or more service providers.

2. ensure that a sufficient amount of users tracking information is disclosed to the competent authorities of the State Party or to a person appointed by these authorities to allow the State Party to determine the service providers and the transmission path of the communications.

7. Search for computer data/information

Article 19(1)(2) Budapest Convention. Search and Seizure of Stored Computer Data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

(*a*) a computer system or part of it and computer data stored therein; and

(*b*) a computer-data storage medium in which computer data may be stored in its territory.

2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

Article 26 League of Arab States Convention. Inspecting Stored Information

1. Every State Party shall commit itself to adopting the procedures necessary to enable its competent authorities to inspect or access:

(*a*) an information technology or part thereof and the information stored therein or thereon.

(*b*) the storage environment or medium in or on which the information may be stored.

2. Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to inspect or access a specific information technology or part thereof in conformity with paragraph 1(a) if it is believed that the required information is stored in another information technology or in part thereof in its territory and such information is legally accessible or available in the first technology, the scope of inspection may be extended and the other technology accessed.

8. Seizure of stored computer data or information

Article 19(3) Budapest Convention. Search and Seizure of Stored Computer Data

3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

(*a*) seize or similarly secure a computer system or part of it or a computer-data storage medium;

(*b*) make and retain a copy of those computer data;

(*c*) maintain the integrity of the relevant stored computer data;

(*d*) render inaccessible or remove those computer data in the accessed computer system.

Article 27(1) League of Arab States Convention. Seizure of Stored Information

1. Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to seize and safeguard information technology information accessed according to Article 26, paragraph 1, of this Convention.

These procedures include the authority to:

(*a*) seize and safeguard the information technology or part thereof or the storage medium for the information technology information.

(*b*) make a copy the information technology information and keep it.

(*c*) maintain the integrity of the stored information technology information.

(*d*) remove such accessed information from the information technology or prevent its access.

2. Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to order any person who is acquainted with the functioning of the information technology or the procedures applied to protect the information technology to give the information necessary to complete the procedures mentioned in paragraphs 2 and 3 of Article 26 of this Convention.

9. Real-time collection of traffic data

Article 20 Budapest Convention. Real-Time Collection of Traffic Data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

(*a*) collect or record through the application of technical means on the territory of that Party, and

(*b*) compel a service provider, within its existing technical capability:

(*i*) to collect or record through the application of technical means on the territory of that Party; or

(*ii*) to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 28 League of Arab States Convention. Expeditious Gathering of Users Tracking Information

1. Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to:

(*a*) gather or register using technical means in the territory of this State Party.

(*b*) require the service provider, within his technical competence, to:

- gather or register using technical means in the territory of this State Party, or
- cooperate with and help the competent authorities to expeditiously gather and register users tracking information with the relevant communications and which are transmitted by means of the information technology.

2. If, because of the domestic legal system, the State Party is unable to adopt the procedures set forth in paragraph 1(a), it may adopt other procedures in the form necessary to ensure the expeditious gathering and registration of users tracking information corresponding to the relevant communications in its territory using the technical means in that territory.

3. Every State Party shall commit itself to adopting the procedures necessary to require the service provider to maintain the secrecy of any information when exercising the authority set forth in this Article.

10. Interception/real-time collection of content data

Article 21 Budapest Convention. Interception of Content Data

1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

(*a*) collect or record through the application of technical means on the territory of that Party, and

(*b*) compel a service provider, within its existing technical capability:

(*i*) to collect or record through the application of technical means on the territory of that Party, or

(*ii*) to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 29 League of Arab States Convention. Interception of Content Information

1. Every State Party shall commit itself to adopting the legislative procedures necessary as regards a series of offences set forth in the domestic law, in order to enable the competent authorities to:

(*a*) gather or register through technical means in the territory of this State Party, or

(*b*) cooperate with and help the competent authorities to expeditiously gather and register content information of the relevant communications in its territory and which are transmitted by means of the information technology.

2. If, because of the domestic legal system, the State Party is unable to adopt the procedures set forth in paragraph 1(a), it may adopt other procedures in the form necessary to ensure the expeditious gathering and registration of content information corresponding to the relevant communications in its territory using the technical means in that territory.

3. Every State Party shall commit itself to adopting the procedures necessary to require the service provider to maintain the secrecy of any information when exercising the authority set forth in this Article.

11. Provision of assistance

Article 19(4) Budapest Convention. Search and Seizure of Stored Computer Data

4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

Article 27(2) League of Arab States Convention. Seizure of Stored Information

2. Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to order any person who is acquainted with the functioning of the information technology or the procedures applied to protect the information technology to give the information necessary to complete the procedures mentioned in paragraphs 2 and 3 of Article 26 of this Convention.

F. Specialisation of, Training for, and Cooperation with National Authorities

Paragraph 11 IEG Recommendations

Member States should foster efforts to build the capacity of law enforcement personnel, including those working in specialized law enforcement structures, prosecutors and the judiciary, so that such personnel possess at least basic technical knowledge of electronic evidence and are able to respond effectively and expeditiously to requests for assistance in the tracing of communications and undertake other measures necessary for the investigation of cybercrime.

Paragraph 15 IEG Recommendations

In legal systems that use the inquisitorial model, where judicial officers are also investigators, the judiciary should receive specialized training on cybercrime.

Paragraph 29 IEG Recommendations

Sustainable capacity-building and technical assistance to increase capabilities across operational areas and strengthen the capacity of national authorities to respond to cybercrime should be prioritized and increased, including through networking, joint meetings and training, the sharing of best practices, training materials, and templates for cooperation. Such capacity-building and training should include highly specialized training for practitioners that promotes, in particular, the participation of female experts, and should address the needs of legislators and policymakers to better handle issues of data retention for law enforcement purposes. The capacity-building and training should also be focused on improving the abilities of law enforcement authorities, investigators and analysts in forensics, in the use of open source data for investigations and in the chain of custody for electronic evidence, as well as in collecting and sharing electronic evidence abroad. Another focus of the capacity-building and training should be on improving the abilities of judges, prosecutors, central authorities and lawyers to effectively adjudicate and deal with relevant cases.

Paragraph 43 IEG Recommendations

States should provide training for specialized magistrates and judges who handle cybercrime cases and provide investigative bodies with high-performance tools for tracing cryptocurrencies and addressing their use for criminal purposes.

Paragraph 62 IEG Recommendations

It was recommended that States invest in capacity-building to upgrade the skills of officers from the whole spectrum of the criminal justice system as an efficient preventive measure of deterrent effect against cybercrime.

1. Specialized authorities (in particular for law enforcement)

Paragraph 34 IEG Recommendations

Member States should consider investing in specialized centralized cybercrime forces and in regional technological units for criminal investigations.

Paragraph 35 IEG Recommendations

Member States should also consider establishing separate cybercrime units within central authorities for mutual legal assistance as a base of expertise in the complex area of international cooperation. Such specialized units not only provide benefit in the day-to-day practice of mutual legal assistance, but also allow for focused capacity-building assistance such as training to address the needs of domestic and foreign authorities on how to obtain mutual legal assistance involving electronic evidence quickly and efficiently in cyber-related matters.

Article 25(2) AU Convention 2014. Legal Measures

2. National Regulatory Authorities

Each State Party shall adopt such legislative and/or regulatory measures as it deems necessary to confer specific responsibility on institutions, either newly established or pre-existing, as well as on the designated officials of the said institutions, with a view to conferring on them a statutory authority and legal capacity to act in all aspects of cyber security application, including but not limited to response to cyber security incidents, and coordination and cooperation in the field of restorative justice, forensic investigations, prosecutions, etc.

Article 36 UNCAC. Specialized Authorities

Each State Party shall, in accordance with the fundamental principles of its legal system, ensure the existence of a body or bodies or persons specialized in combating

corruption through law enforcement. Such body or bodies or persons shall be granted the necessary independence, in accordance with the fundamental principles of the legal system of the State Party, to be able to carry out their functions effectively and without any undue influence. Such persons or staff of such body or bodies should have the appropriate training and resources to carry out their tasks.

2. Measures to enhance cooperation with law enforcement authorities

Article 26 UNTOC. Measures to Enhance Cooperation with Law Enforcement Authorities

1. Each State Party shall take appropriate measures to encourage persons who participate or who have participated in organized criminal groups:

(*a*) To supply information useful to competent authorities for investigative and evidentiary purposes on such matters as:

(*i*) The identity, nature, composition, structure, location or activities of organized criminal groups;

(*ii*) Links, including international links, with other organized criminal groups;

(*iii*) Offences that organized criminal groups have committed or may commit;

(*b*) To provide factual, concrete help to competent authorities that may contribute to depriving organized criminal groups of their resources or of the proceeds of crime.

2. Each State Party shall consider providing for the possibility, in appropriate cases, of mitigating punishment of an accused person who provides substantial cooperation in the investigation or prosecution of an offence covered by this Convention.

3. Each State Party shall consider providing for the possibility, in accordance with fundamental principles of its domestic law, of granting immunity from prosecution to a person who provides substantial cooperation in the investigation or prosecution of an offence covered by this Convention.

4. Protection of such persons shall be as provided for in article 24 of this Convention.

5. Where a person referred to in paragraph 1 of this article located in one State Party can provide substantial cooperation to the competent authorities of another State Party, the States Parties concerned may consider entering into agreements or arrangements, in accordance with their domestic law, concerning the potential provision by the other State Party of the treatment set forth in paragraphs 2 and 3 of this article.

Article 37 UNCAC. Cooperation with law enforcement authorities

1. Each State Party shall take appropriate measures to encourage persons who participate or who have participated in the commission of an offence established in accordance with this Convention to supply information useful to competent authorities for investigative and evidentiary purposes and to provide factual, specific help to competent authorities that may contribute to depriving offenders of the proceeds of crime and to recovering such proceeds.

2. Each State Party shall consider providing for the possibility, in appropriate cases, of mitigating punishment of an accused person who provides substantial cooperation in the investigation or prosecution of an offence established in accordance with this Convention.

3. Each State Party shall consider providing for the possibility, in accordance with fundamental principles of its domestic law, of granting immunity from prosecution to a person who provides substantial cooperation in the investigation or prosecution of an offence established in accordance with this Convention.

4. Protection of such persons shall be, mutatis mutandis, as provided for in article 32 of this Convention.

5. Where a person referred to in paragraph 1 of this article located in one State Party can provide substantial cooperation to the competent authorities of another State Party, the States Parties concerned may consider entering into agreements or arrangements, in accordance with their domestic law, concerning the potential provision by the other State Party of the treatment set forth in paragraphs 2 and 3 of this article.

3. Cooperation between national authorities for investigating and prosecuting criminal offences

Article 38 UNCAC. Cooperation Between National Authorities

Each State Party shall take such measures as may be necessary to encourage, in accordance with its domestic law, cooperation between, on the one hand, its public authorities, as well as its public officials, and, on the other hand, its authorities responsible for investigating and prosecuting criminal offences. Such cooperation may include:

(*a*) Informing the latter authorities, on their own initiative, where there are reasonable grounds to believe that any of the offences established in accordance with articles 15, 21 and 23 of this Convention has been committed; or

(*b*) Providing, upon request, to the latter authorities all necessary information.

4. Cooperation between national authorities and the private sector

Paragraph 22 IEG Recommendations

Countries are encouraged to streamline cooperation with industry and enhance collaboration between the Government and private service providers, in particular for addressing the challenges posed by harmful criminal material on the Internet.

Paragraph 57 IEG Recommendations

Industry is a key partner in preventing cybercrime. Countries should consider implementing mechanisms for cooperating with industry, including on referrals to competent national authorities and takedowns of harmful criminal material, including child sexual exploitation and abhorrent violent material.

Article 39 UNCAC. Cooperation Between National Authorities and the Private Sector

1. Each State Party shall take such measures as may be necessary to encourage, in accordance with its domestic law, cooperation between national investigating and prosecuting authorities and entities of the private sector, in particular financial institutions, relating to matters involving the commission of offences established in accordance with this Convention.

2. Each State Party shall consider encouraging its nationals and other persons with a habitual residence in its territory to report to the national investigating and prosecuting authorities the commission of an offence established in accordance with this Convention.

Article 26(3) AU Convention 2014. National Cyber Security System

3. Public-Private Partnership

Each State Party shall develop public-private partnership as a model to engage industry, the civil society, and academia in the promotion and enhancement of a culture of cyber security.

5. Training of relevant national personnel

Article 29(1) UNTOC. Training and Technical Assistance

1. Each State Party shall, to the extent necessary, initiate, develop or improve specific training programmes for its law enforcement personnel, including prosecutors, investigating magistrates and customs personnel, and other personnel charged with the prevention, detection and control of the offences covered by this Convention. Such programmes may include secondments and exchanges of staff. Such programmes shall deal, in particular and to the extent permitted by domestic law, with the following:

(*a*) Methods used in the prevention, detection and control of the offences covered by this Convention;

(*b*) Routes and techniques used by persons suspected of involvement in offences covered by this Convention, including in transit States, and appropriate countermeasures;

(*c*) Monitoring of the movement of contraband;

(*d*) Detection and monitoring of the movements of proceeds of crime, property, equipment or other instrumentalities and methods used for the transfer, concealment or disguise of such proceeds, property, equipment or other instrumentalities, as well as methods used in combating money-laundering and other financial crimes;

(*e*) Collection of evidence;

(*f*) Control techniques in free trade zones and free ports;

(*g*) Modern law enforcement equipment and techniques, including electronic surveillance, controlled deliveries and undercover operations;

(*h*) Methods used in combating transnational organized crime committed through the use of computers, telecommunications networks or other forms of modern technology; and

(*i*) Methods used in the protection of victims and witnesses.

Article 60(1) UNCAC. Training and Technical Assistance

1. Each State Party shall, to the extent necessary, initiate, develop or improve specific training programmes for its personnel responsible for preventing and combating corruption. Such training programmes could deal, inter alia, with the following areas:

(*a*) Effective measures to prevent, detect, investigate, punish and control corruption, including the use of evidence-gathering and investigative methods;

(*b*) Building capacity in the development and planning of strategic anticorruption policy;

(*c*) Training competent authorities in the preparation of requests for mutual legal assistance that meet the requirements of this Convention;

(*d*) Evaluation and strengthening of institutions, public service management and the management of public finances, including public procurement, and the private sector;

(*e*) Preventing and combating the transfer of proceeds of offences established in accordance with this Convention and recovering such proceeds;

(*f*) Detecting and freezing of the transfer of proceeds of offences established in accordance with this Convention;

(*g*) Surveillance of the movement of proceeds of offences established in accordance with this Convention and of the methods used to transfer, conceal or disguise such proceeds;

(*h*) Appropriate and efficient legal and administrative mechanisms and methods for facilitating the return of proceeds of offences established in accordance with this Convention;

(*i*) Methods used in protecting victims and witnesses who cooperate with judicial authorities; and

(*j*) Training in national and international regulations and in languages.

Article 26(4) AU Convention. National Cyber Security System

4. Education and training

Each State Party shall adopt measures to develop capacity building with a view to offering training which covers all areas of cyber security to different stakeholders, and setting standards for the private sector.

States Parties undertake to promote technical education for information and communication technology professionals, within and outside governmental bodies, through certification and standardization of training; categorization of professional qualifications as well as development and needs-based distribution of educational material.

6. Training and education for the public

Paragraph 9 IEG Recommendations

Countries should invest in raising awareness of cybercrime among the general public and private industry in order to address the lower rates of reporting of cybercrime compared with other types of crime.

Paragraph 42 IEG Recommendations

Preventive activities must be proactive, regular, continuous and suitable for vulnerable groups.

Paragraph 45 IEG Recommendations

Member States are encouraged to continue to include effective prevention measures at national and international levels and to focus on proactive activities such as raising awareness about the risks of cybercrime, targeting such campaigns at modi operandi such as phishing or malware (“ransomware”) and at different groups such as youth and elderly people. Member States are also encouraged to continue to focus on the likelihood or prosecution and punishment of offenders and efforts to prevent crime by identifying and disrupting ongoing illicit activities online. Police and public prosecution services should invest in signalling, detecting and reacting to cybercrime threats. Public-private partnership is indispensable. These prevention activities do not require extra laws or regulations.

Paragraph 54 IEG Recommendations

States should support businesses and communities in raising awareness of cybercrime risks, mitigation strategies and enhancing cyberpractices, as these can have significant downstream preventive benefits.

Paragraph 58 IEG Recommendations

Regular advisories on incident prevention should be issued and shared with users, organizations and other stakeholders to enable them to prevent cyber-incidents that could potentially lead to criminal activities.

Article 26(2)(4) AU Convention 2014. National Cyber Security System

2. Role of Governments

Each State Party shall undertake to provide leadership for the development of the cyber security culture within its borders. Member States undertake to sensitize, provide education and training, and disseminate information to the public.

4. Education and training

Each State Party shall adopt measures to develop capacity building with a view to offering training which covers all areas of cyber security to different stakeholders and setting standards for the private sector.

States Parties undertake to promote technical education for information and communication technology professionals, within and outside government bodies, through certification and standardization of training; categorization of professional qualifications as well as development and needs-based distribution of educational material.

7. Conference of the parties to the convention and mechanism to review its implementation

Article 32 UNTOC. Conference of the Parties to the Convention

1. A Conference of the Parties to the Convention is hereby established to improve the capacity of States Parties to combat transnational organized crime and to promote and review the implementation of this Convention.

2. The Secretary-General of the United Nations shall convene the Conference of the Parties not later than one year following the entry into force of this Convention. The Conference of the Parties shall adopt rules of procedure and rules governing the activities set forth in paragraphs 3 and 4 of this article (including rules concerning payment of expenses incurred in carrying out those activities).

3. The Conference of the Parties shall agree upon mechanisms for achieving the objectives mentioned in paragraph 1 of this article, including:

(*a*) Facilitating activities by States Parties under articles 29, 30 and 31 of this Convention, including by encouraging the mobilization of voluntary contributions;

(*b*) Facilitating the exchange of information among States Parties on patterns and trends in transnational organized crime and on successful practices for combating it;

(*c*) Cooperating with relevant international and regional organizations and non-governmental organizations;

(*d*) Reviewing periodically the implementation of this Convention;

(*e*) Making recommendations to improve this Convention and its implementation.

4. For the purpose of paragraphs 3 (d) and (e) of this article, the Conference of the Parties shall acquire the necessary knowledge of the measures taken by States Parties in implementing this Convention and the difficulties encountered by them in doing so through information provided by them and through such supplemental review mechanisms as may be established by the Conference of the Parties.

5. Each State Party shall provide the Conference of the Parties with information on its programmes, plans and practices, as well as legislative and administrative measures to implement this Convention, as required by the Conference of the Parties.

Article 63 UNCAC. Conference of the States Parties to the Convention

1. A Conference of the States Parties to the Convention is hereby established to improve the capacity of and cooperation between States Parties to achieve the objectives set forth in this Convention and to promote and review its implementation.

2. The Secretary-General of the United Nations shall convene the Conference of the States Parties not later than one year following the entry into force of this Convention. Thereafter, regular meetings of the Conference of the States Parties shall be held in accordance with the rules of procedure adopted by the Conference.

3. The Conference of the States Parties shall adopt rules of procedure and rules governing the functioning of the activities set forth in this article, including rules concerning the admission and participation of observers, and the payment of expenses incurred in carrying out those activities.

4. The Conference of the States Parties shall agree upon activities, procedures and methods of work to achieve the objectives set forth in paragraph 1 of this article, including:

(*a*) Facilitating activities by States Parties under articles 60 and 62 and chapters II to V of this Convention, including by encouraging the mobilization of voluntary contributions;

(*b*) Facilitating the exchange of information among States Parties on patterns and trends in corruption and on successful practices for preventing and combating it and for the return of proceeds of crime, through, inter alia, the publication of relevant information as mentioned in this article;

(*c*) Cooperating with relevant international and regional organizations and mechanisms and non-governmental organizations;

(*d*) Making appropriate use of relevant information produced by other international and regional mechanisms for combating and preventing corruption in order to avoid unnecessary duplication of work;

(*e*) Reviewing periodically the implementation of this Convention by its States Parties;

(*f*) Making recommendations to improve this Convention and its implementation;

(*g*) Taking note of the technical assistance requirements of States Parties with regard to the implementation of this Convention and recommending any action it may deem necessary in that respect.

5. For the purpose of paragraph 4 of this article, the Conference of the States Parties shall acquire the necessary knowledge of the measures taken by States Parties in implementing this Convention and the difficulties encountered by them in doing so through information provided by them and through such supplemental review mechanisms as may be established by the Conference of the States Parties.

6. Each State Party shall provide the Conference of the States Parties with information on its programmes, plans and practices, as well as on legislative and administrative measures to implement this Convention, as required by the Conference of the States Parties. The Conference of the States Parties shall examine the most effective way of receiving and acting upon information, including, inter alia, information received from States Parties and from competent international organizations. Inputs received from relevant non-governmental organizations duly accredited in accordance with procedures to be decided upon by the Conference of the States Parties may also be considered.

7. Pursuant to paragraphs 4 to 6 of this article, the Conference of the States Parties shall establish, if it deems it necessary, any appropriate mechanism or body to assist in the effective implementation of the Convention.

8. Secretariat

Article 33 UNTOC. Secretariat

1. The Secretary-General of the United Nations shall provide the necessary secretariat services to the Conference of the Parties to the Convention.

2. The secretariat shall:

(*a*) Assist the Conference of the Parties in carrying out the activities set forth in article 32 of this Convention and make arrangements and provide the necessary services for the sessions of the Conference of the Parties;

(*b*) Upon request, assist States Parties in providing information to the Conference of the Parties as envisaged in article 32, paragraph 5, of this Convention; and

(*c*) Ensure the necessary coordination with the secretariats of relevant international and regional organizations.

Article 64 UNCAC. Secretariat

1. The Secretary-General of the United Nations shall provide the necessary secretariat services to the Conference of the States Parties to the Convention.

2. The secretariat shall:

(*a*) Assist the Conference of the States Parties in carrying out the activities set forth in article 63 of this Convention and make arrangements and provide the necessary services for the sessions of the Conference of the States Parties;

(*b*) Upon request, assist States Parties in providing information to the Conference of the States Parties as envisaged in article 63, paragraphs 5 and 6, of this Convention; and

(*c*) Ensure the necessary coordination with the secretariats of relevant international and regional organizations.

9. Consultations of the Parties

Article 46 Budapest Convention. Consultations of the Parties

1. The Parties shall, as appropriate, consult periodically with a view to facilitating:

(*a*) the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

(*b*) the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

(*c*) consideration of possible supplementation or amendment of the Convention.

2. The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3. The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4. Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5. The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

Article 5(2-4) SCO Agreement. Main Formats and Mechanisms of Cooperation

2. For the purpose of reviewing the implementation of this Agreement, exchange of information, analysis and joint assessment of emerging threats to information security, as well as identification, reconciliation and coordination of joint responses to these threats, the Parties on a regular basis shall hold consultations of the authorized representatives of the Parties and competent authorities of the Parties (hereinafter – the "consultations").

Regular consultations shall be held by agreement between the Parties, as a rule, once every six months in the Secretariat of the Shanghai Cooperation Organization, or in the territory of one of the Parties at its invitation.

Any Party may initiate early consultations by, offering time and place, as well as the agenda to be subsequently agreed by all the Parties and the Secretariat of the Shanghai Cooperation Organization.

3. Practical collaboration in specific areas of cooperation envisaged by this Agreement may be carried out by the Parties through the competent authorities of the Parties responsible for the implementation of the Agreement.

4. In order to create the legal and institutional framework or cooperation in specific areas, the competent authorities of the Parties may conclude appropriate interdepartmental agreements.

G. Protection of Human Rights and Fundamental Freedoms

1. Conditions and safeguards

Paragraph 21 IEG Recommendations

Countries are called upon to pay particular attention to the necessary proportionality of investigative measures, while respecting fundamental freedoms and the personal data protection regimes associated with private correspondence.

Article 25(3) AU Convention 2014. Legal Measures

3. Rights of citizens

In adopting legal measures in the area of cyber security and establishing the framework for implementation thereof, each State Party shall ensure that the measures so adopted will not infringe on the rights of citizens guaranteed under the national constitution and internal laws, and protected by international conventions, particularly the African Charter on Human and Peoples' Rights, and other basic rights such as freedom of expression, the right to privacy and the right to a fair hearing, among others.

Article 15 Budapest Convention. Conditions and Safeguards

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent

supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

2. Safeguards related to international law in general

Article 33 AU Convention 2014. Safeguard Provisions

The provisions of this Convention shall not be interpreted in a manner that is inconsistent with the relevant principles of international law, including international customary law.

H. Electronic Evidence/Admissibility of Electronic Evidence/Records

Paragraph 12 IEG Recommendations

Member States should take necessary measures to enact legislation that ensures the admissibility of electronic evidence, bearing in mind that admissibility of evidence, including electronic evidence, is an issue that each country should address according to its domestic law.

Paragraph 16 IEG Recommendations

States may consider establishing the following data as electronic evidence in their domestic legislation: traffic data, such as log files; content data, such as emails; subscriber data, such as user registration information; and other data that are stored, processed and transmitted in a digital format and are produced during the commission of a crime and can therefore be used to prove the facts of that crime.

Paragraph 18 IEG Recommendations

Member States should make efforts to enhance cooperation in gathering electronic evidence. In this regard, they are encouraged to consider, inter alia, the following:

(*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*) Strengthening of the technical and legal capacities of law enforcement agencies, judges and prosecutors through capacity-building and skill development programmes;

(*g*) Holding of workshops and seminars to raise awareness of best practices in addressing cybercrime.

Article 29(4) AU Convention 2014. Offences Specific to Information and Communication Technologies

4. Offences relating to electronic message security measures

State Parties shall take the necessary legislative and/or regulatory measures to ensure that digital evidence in criminal cases is admissible to establish offenses under national criminal law, provided such evidence has been presented during proceedings and discussed before the judge, that the person from whom it originates can be duly identified, and that it has been made out and retained in a manner capable of assuring its integrity.

I. International Cooperation

Paragraph 8 IEG Recommendations

Countries should devote resources to developing expertise to investigate cybercrime and to creating partnerships that employ cooperation mechanisms to obtain vital evidence.

Paragraph 19 IEG Recommendations

The efficiency of international cooperation should be improved by establishing rapid response mechanisms for international cooperation, as well as channels of communication through liaison officers and information technology systems between national authorities for the cross-border collection of evidence and online transfer of electronic evidence.

Paragraph 20 IEG Recommendations

The procedures for international cooperation should be optimized so that maximum assistance is provided within the possibilities derived from domestic legal frameworks for international cooperation requests concerning preservation of electronic evidence and access to log files and user registration information in a way that does not interfere with human rights and fundamental freedoms or property rights.

Paragraph 28 IEG Recommendations

Effective international cooperation requires national laws that create procedures that enable international cooperation. Thus, national laws must permit international cooperation among law enforcement agencies.

Paragraph 30 IEG Recommendations

International cooperation is important for gathering and sharing electronic evidence in the context of cross-border investigations and for fast and effective responses to requests for mutual legal assistance related to preserving and obtaining electronic evidence. The principles of sovereignty and reciprocity should be respected in the process.

1. General principles relating to international cooperation

Article 23 Budapest Convention. General Principles Relating to International Co-Operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Article 5 Dushanbe Agreement. Forms of Cooperation

The competent authorities of the Parties shall, within the framework of this Agreement, cooperate in the following forms:

(*a*) Exchange of information, including:

Information about the crimes in the field of information technologies being prepared or committed and the individuals and legal entities involved;

On the forms and methods of prevention, detection, suppression, solving and investigation of crimes in this area;

On the methods of committing crimes in the field of information technologies;

On the national legislation and international treaties of the Parties governing the prevention, detection, interdiction, solving and investigation of crimes in the field of information technologies;

(*b*) Execution of requests for assistance in obtaining information that may contribute to the prevention, detection, suppression, solving and investigation of a crime committed against a citizen of the requesting Party or in the territory of the requesting Party, for the conduct of investigative measures;

(*c*) Planning and carrying out coordinated activities and operations to prevent, detect, suppress, solve and investigate crimes in the field of information technologies;

(*d*) Assistance in training and professional development, including through internships, conferences, seminars and training courses;

(*e*) Creation of information systems and software products that ensure the performance of tasks for the prevention, detection, suppression, solving and investigation of crimes in the field of information technologies;

(*f*) Exchange of publications and research findings, as well as joint research on problems of mutual interest in combating crimes in the field of information technologies;

(*g*) Exchange of normative legal acts, scientific and technical literature on combating crimes in the field of information technologies;

(*h*) Exchange of software products and solutions used in the prevention, detection, interdiction, solving and investigation of crimes in the field of information technologies through cooperation and exchange of experience;

(*i*) Responding to a request for urgent preservation of data stored on computer systems;

(*j*) Other mutually acceptable forms.

2. International cooperation in criminal matters

Article 43 UNCAC. International Cooperation

1. States Parties shall cooperate in criminal matters in accordance with articles 44 to 50 of this Convention. Where appropriate and consistent with their domestic legal system, States Parties shall consider assisting each other in investigations of and proceedings in civil and administrative matters relating to corruption.

2. In matters of international cooperation, whenever dual criminality is considered a requirement, it shall be deemed fulfilled irrespective of whether the laws of the requested State Party place the offence within the same category of offence or denominate the offence by the same terminology as the requesting State Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under the laws of both States Parties.

3. Extradition

Article 16 UNTOC. Extradition

1. This article shall apply to the offences covered by this Convention or in cases where an offence referred to in article 3, paragraph 1 (a) or (b), involves organized criminal group and the person who is the subject of the request for extradition is located in the territory of the requested State Party, provided that the offence for which extradition is sought is punishable under the domestic law of both the requesting State Party and the requested State Party.

2. If the request for extradition includes several separate serious crimes, some of which are not covered by this article, the requested State Party may apply this article also in respect of the latter offences.

3. Each of the offences to which this article applies shall be deemed to be included as an extraditable offence in any extradition treaty existing between States Parties. States Parties undertake to include such offences as extraditable offences in every extradition treaty to be concluded between them.

4. If a State Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another State Party with which it has no extradition treaty, it may consider this Convention the legal basis for extradition in respect of any offence to which this article applies.

5. States Parties that make extradition conditional on the existence of a treaty shall:

(*a*) At the time of deposit of their instrument of ratification, acceptance, approval of or accession to this Convention, inform the Secretary-General of the United Nations whether they will take this Convention as the legal basis for cooperation on extradition with other States Parties to this Convention; and

(*b*) If they do not take this Convention as the legal basis for cooperation on extradition, seek, where appropriate, to conclude treaties on extradition with other States Parties to this Convention in order to implement this article.

6. States Parties that do not make extradition conditional on the existence of a treaty shall recognize offences to which this article applies as extraditable offences between themselves.

7. Extradition shall be subject to the conditions provided for by the domestic law of the requested State Party or by applicable extradition treaties, including, inter alia, conditions in relation to the minimum penalty requirement for extradition and the grounds upon which the requested State Party may refuse extradition.

8. States Parties shall, subject to their domestic law, endeavour to expedite extradition procedures and to simplify evidentiary requirements relating thereto in respect of any offence to which this article applies.

9. Subject to the provisions of its domestic law and its extradition treaties, the requested State Party may, upon being satisfied that the circumstances so warrant and are urgent and at the request of the requesting State Party, take a person whose extradition is sought and who is present in its territory into custody or take other appropriate measures to ensure his or her presence at extradition proceedings.

10. A State Party in whose territory an alleged offender is found, if it does not extradite such person in respect of an offence to which this article applies solely on the ground that he or she is one of its nationals, shall, at the request of the State Party seeking extradition, be obliged to submit the case without undue delay to its competent authorities for the purpose of prosecution. Those authorities shall take their decision and conduct their proceedings in the same manner as in the case of any other offence of a grave nature under the domestic law of that State Party. The States Parties concerned shall cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecution.

11. Whenever a State Party is permitted under its domestic law to extradite or otherwise surrender one of its nationals only upon the condition that the person will be returned to that State Party to serve the sentence imposed as a result of the trial or proceedings for which the extradition or surrender of the person was sought and that State Party and the State Party seeking the extradition of the person agree with this option and other terms that they may deem appropriate, such conditional extradition or surrender shall be sufficient to discharge the obligation set forth in paragraph 10 of this article.

12. If extradition, sought for purposes of enforcing a sentence, is refused because the person sought is a national of the requested State Party, the requested Party shall, if its domestic law so permits and in conformity with the requirements of such law, upon application of the requesting Party, consider the enforcement of the sentence that has been imposed under the domestic law of the requesting Party or the remainder thereof.

13. Any person regarding whom proceedings are being carried out in connection with any of the offences to which this article applies shall be guaranteed fair treatment at all stages of the proceedings, including enjoyment of all the rights and guarantees provided by the domestic law of the State Party in the territory of which that person is present.

14. Nothing in this Convention shall be interpreted as imposing an obligation to extradite if the requested State Party has substantial grounds for believing that the request has been made for the purpose of prosecuting or punishing a person on account of that person's sex, race, religion, nationality, ethnic origin or political opinions or that compliance with the request would cause prejudice to that person's position for any one of these reasons.

15. States Parties may not refuse a request for extradition on the sole ground that the offence is also considered to involve fiscal matters.

16. Before refusing extradition, the requested State Party shall, where appropriate, consult with the requesting State Party to provide it with ample opportunity to present its opinions and to provide information relevant to its allegation.

17. States Parties shall seek to conclude bilateral and multilateral agreements or arrangements to carry out or to enhance the effectiveness of extradition.

Article 44 UNCAC. Extradition

1. This article shall apply to the offences established in accordance with this Convention where the person who is the subject of the request for extradition is present in the territory of the requested State Party, provided that the offence for which extradition is sought is punishable under the domestic law of both the requesting State Party and the requested State Party.

2. Notwithstanding the provisions of paragraph 1 of this article, a State Party whose law so permits may grant the extradition of a person for any of the offences covered by this Convention that are not punishable under its own domestic law.

3. If the request for extradition includes several separate offences, at least one of which is extraditable under this article and some of which are not extraditable by reason of their period of imprisonment but are related to offences established in accordance with this Convention, the requested State Party may apply this article also in respect of those offences.

4. Each of the offences to which this article applies shall be deemed to be included as an extraditable offence in any extradition treaty existing between States Parties. States Parties undertake to include such offences as extraditable offences in every extradition treaty to be concluded between them. A State Party whose law so permits, in case it uses this Convention as the basis for extradition, shall not consider any of the offences established in accordance with this Convention to be a political offence.

5. If a State Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another State Party with which it has no extradition treaty, it may consider this Convention the legal basis for extradition in respect of any offence to which this article applies.

6. A State Party that makes extradition conditional on the existence of a treaty shall:

(*a*) At the time of deposit of its instrument of ratification, acceptance or approval of or accession to this Convention, inform the Secretary-General of the United Nations whether it will take this Convention as the legal basis for cooperation on extradition with other States Parties to this Convention; and

(*b*) If it does not take this Convention as the legal basis for cooperation on extradition, seek, where appropriate, to conclude treaties on extradition with other States Parties to this Convention in order to implement this article.

7. States Parties that do not make extradition conditional on the existence of a treaty shall recognize offences to which this article applies as extraditable offences between themselves.

8. Extradition shall be subject to the conditions provided for by the domestic law of the requested State Party or by applicable extradition treaties, including, inter alia, conditions in relation to the minimum penalty requirement for extradition and the grounds upon which the requested State Party may refuse extradition.

9. States Parties shall, subject to their domestic law, endeavour to expedite extradition procedures and to simplify evidentiary requirements relating thereto in respect of any offence to which this article applies.

10. Subject to the provisions of its domestic law and its extradition treaties, the requested State Party may, upon being satisfied that the circumstances so warrant and are urgent and at the request of the requesting State Party, take a person whose extradition is sought and who is present in its territory into custody or take other appropriate measures to ensure his or her presence at extradition proceedings.

11. A State Party in whose territory an alleged offender is found, if it does not extradite such person in respect of an offence to which this article applies solely on the ground that he or she is one of its nationals, shall, at the request of the State Party seeking extradition, be obliged to submit the case without undue delay to its competent authorities for the purpose of prosecution. Those authorities shall take their decision and conduct their proceedings in the same manner as in the case of any other offence of a grave nature under the domestic law of that State Party. The States Parties concerned shall cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecution.

12. Whenever a State Party is permitted under its domestic law to extradite or otherwise surrender one of its nationals only upon the condition that the person will be returned to that State Party to serve the sentence imposed as a result of the trial or proceedings for which the extradition or surrender of the person was sought and that State Party and the State Party seeking the extradition of the person agree with this option and other terms that they may deem appropriate, such conditional extradition or surrender shall be sufficient to discharge the obligation set forth in paragraph 11 of this article.

13. If extradition, sought for purposes of enforcing a sentence, is refused because the person sought is a national of the requested State Party, the requested State Party shall, if its domestic law so permits and in conformity with the requirements of such law, upon application of the requesting State Party, consider the enforcement of the sentence imposed under the domestic law of the requesting State Party or the remainder thereof.

14. Any person regarding whom proceedings are being carried out in connection with any of the offences to which this article applies shall be guaranteed fair treatment

at all stages of the proceedings, including enjoyment of all the rights and guarantees provided by the domestic law of the State Party in the territory of which that person is present.

15. Nothing in this Convention shall be interpreted as imposing an obligation to extradite if the requested State Party has substantial grounds for believing that the request has been made for the purpose of prosecuting or punishing a person on account of that person's sex, race, religion, nationality, ethnic origin or political opinions or that compliance with the request would cause prejudice to that person's position for any one of these reasons.

16. States Parties may not refuse a request for extradition on the sole ground that the offence is also considered to involve fiscal matters.

17. Before refusing extradition, the requested State Party shall, where appropriate, consult with the requesting State Party to provide it with ample opportunity to present its opinions and to provide information relevant to its allegation.

18. States Parties shall seek to conclude bilateral and multilateral agreements or arrangements to carry out or to enhance the effectiveness of extradition.

Article 24 Budapest Convention. Extradition

1. (*a*) This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

(*b*) Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2. The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4. Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6. If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7. (*a*) Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible

for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

(*b*) The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Article 31 League of Arab States Convention. Extradition

1. (*a*) This Article applies to the exchange of offenders between State Parties for offences set forth in Chapter II of this Convention, provided that such offences shall be punishable under the laws of the concerned State Parties by deprivation of freedom for a minimum period of one year or a more severe penalty.

(*b*) If a different, less severe, penalty is applicable by virtue of an agreed arrangement or by virtue of the extradition treaty, then the less severe penalty shall apply.

2. Offences set forth in paragraph 1 of this article shall be deemed offences whose perpetrators are extraditable under any extradition treaty between State Parties.

3. If a State Party makes extradition conditional on the existence of a treaty, and it receives an extradition request from a State Party that has no extradition treaty, this Convention may be considered as a legal basis for extradition as regards offences set forth in paragraph 1 of this Article.

4. State Parties that do not require the existence of an extradition treaty shall consider that the offences set forth in paragraph 1 of this Article are offences whose perpetrators are extraditable among such States.

5. Extradition shall be subject to the requirements set forth in the law of the State Party to which the request is submitted or to the applicable extradition treaties, including the grounds on which the State Party can rely to refuse extradition.

6. A contracting State Party may refuse to extradite its nationals and undertake, within the limits of its jurisdiction, to prosecute those of whom who commit in any other State Party offences punishable under the law in both countries by deprivation of freedom for a period of one year or a more severe penalty in any of the two contracting Parties, provided the other State Party addresses to it a prosecution request together with the files, documents, objects and information that it has in its possession. The requesting State Party shall be informed of what is being done regarding its request. Nationality shall be determined at the date the offence happened for which extradition is requested.

7. (*a*) Every State Party shall commit itself to communicate, at the time of signature or deposit of the instrument of ratification or acceptance, the name and address of the authority responsible for extradition or procedural arrest, in the absence of a treaty, to the General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers.

(*b*) The General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers shall establish and update the registry of concerned authorities in the State Parties. Every State Party shall insure that the registry's details are correct at all times.

4. Transfer of sentenced persons

Article 17 UNTOC. Transfer of Sentenced Persons

States Parties may consider entering into bilateral or multilateral agreements or arrangements on the transfer to their territory of persons sentenced to imprisonment or other forms of deprivation of liberty for offences covered by this Convention, in order that they may complete their sentences there.

Article 45 UNCAC. Transfer of Sentenced Persons

States Parties may consider entering into bilateral or multilateral agreements or arrangements on the transfer to their territory of persons sentenced to imprisonment or other forms of deprivation of liberty for offences established in accordance with this Convention in order that they may complete their sentences there.

5. Mutual legal assistance

Paragraph 25 IEG Recommendations

Member States should establish practices that allow the transmittal and receipt of mutual legal assistance requests through electronic means to reduce delays in the State-to-State transmission of documents.

Paragraph 32 IEG Recommendations

UNODC has developed the Mutual Legal Assistance Request Writer Tool to assist criminal justice practitioners in drafting mutual legal assistance requests. The Office has also developed the *Practical Guide for Requesting Electronic Evidence Across Borders,* available on request to government practitioners in Member States. Countries may benefit from employing those key tools developed by UNODC.

Paragraph 37 IEG Recommendations

Member States should be reminded to utilize central authorities in transmitting requests for mutual legal assistance and in working with competent authorities for the execution of such requests to ensure compliance with existing treaties and to reduce delays in the process.

Article 28(2) AU Convention 2014. International Cooperation

2. Mutual legal assistance

State Parties that do not have agreements on mutual assistance in cyber-crime shall undertake to encourage the signing of agreements on mutual legal assistance in conformity with the principle of double criminal liability, while promoting the exchange of information as well as the efficient sharing of data between the organizations of State Parties on a bilateral and multilateral basis.

Article 18 UNTOC. Mutual Legal Assistance

1. States Parties shall afford one another the widest measure of mutual legal assistance in investigations, prosecutions and judicial proceedings in relation to the offences covered by this Convention as provided for in article 3 and shall reciprocally extend to one another similar assistance where the requesting State Party has reasonable grounds to suspect that the offence referred to in article 3, paragraph 1 (a) or (b), is transnational in nature, including that victims, witnesses, proceeds, instrumentalities or evidence of such offences are located in the requested State Party and that the offence involves an organized criminal group.

2. Mutual legal assistance shall be afforded to the fullest extent possible under relevant laws, treaties, agreements and arrangements of the requested State Party with respect to investigations, prosecutions and judicial proceedings in relation to the offences for which a legal person may be held liable in accordance with article 10 of this Convention in the requesting State Party.

3. Mutual legal assistance to be afforded in accordance with this article may be requested for any of the following purposes:

(*a*) Taking evidence or statements from persons;

(*b*) Effecting service of judicial documents;

(*c*) Executing searches and seizures, and freezing;

(*d*) Examining objects and sites;

(*e*) Providing information, evidentiary items and expert evaluations;

(*f*) Providing originals or certified copies of relevant documents and records, including government, bank, financial, corporate or business records;

(*g*) Identifying or tracing proceeds of crime, property, instrumentalities or other things for evidentiary purposes;

(*h*) Facilitating the voluntary appearance of persons in the requesting State Party;

(*i*) Any other type of assistance that is not contrary to the domestic law of the requested State Party.

4. Without prejudice to domestic law, the competent authorities of a State Party may, without prior request, transmit information relating to criminal matters to a competent authority in another State Party where they believe that such information could assist the authority in undertaking or successfully concluding inquiries and criminal proceedings or could result in a request formulated by the latter State Party pursuant to this Convention.

5. The transmission of information pursuant to paragraph 4 of this article shall be without prejudice to inquiries and criminal proceedings in the State of the competent authorities providing the information. The competent authorities receiving the information shall comply with a request that said information remain confidential, even temporarily, or with restrictions on its use. However, this shall not prevent the receiving State Party from disclosing in its proceedings information that is exculpatory to an accused person. In such a case, the receiving State Party shall notify the transmitting State Party prior to the disclosure and, if so requested, consult with the transmitting State Party. If, in an exceptional case, advance notice is not possible, the receiving State Party shall inform the transmitting State Party of the disclosure without delay.

6. The provisions of this article shall not affect the obligations under any other treaty, bilateral or multilateral, that governs or will govern, in whole or in part, mutual legal assistance.

7. Paragraphs 9 to 29 of this article shall apply to requests made pursuant to this article if the States Parties in question are not bound by a treaty of mutual legal assistance. If those States Parties are bound by such a treaty, the corresponding provisions of that treaty shall apply unless the States Parties agree to apply paragraphs 9 to 29 of this article in lieu thereof. States Parties are strongly encouraged to apply these paragraphs if they facilitate cooperation.

8. States Parties shall not decline to render mutual legal assistance pursuant to this article on the ground of bank secrecy.

9. States Parties may decline to render mutual legal assistance pursuant to this article on the ground of absence of dual criminality. However, the requested State Party may, when it deems appropriate, provide assistance, to the extent it decides at its discretion, irrespective of whether the conduct would constitute an offence under the domestic law of the requested State Party.

10. A person who is being detained or is serving a sentence in the territory of one State Party whose presence in another State Party is requested for purposes of identification, testimony or otherwise providing assistance in obtaining evidence for investigations, prosecutions or judicial proceedings in relation to offences covered by this Convention may be transferred if the following conditions are met:

(*a*) The person freely gives his or her informed consent;

(*b*) The competent authorities of both States Parties agree, subject to such conditions as those States Parties may deem appropriate.

11. For the purposes of paragraph 10 of this article:

(*a*) The State Party to which the person is transferred shall have the authority and obligation to keep the person transferred in custody, unless otherwise requested or authorized by the State Party from which the person was transferred;

(*b*) The State Party to which the person is transferred shall without delay implement its obligation to return the person to the custody of the State Party from which the person was transferred as agreed beforehand, or as otherwise agreed, by the competent authorities of both States Parties;

(*c*) The State Party to which the person is transferred shall not require the State Party from which the person was transferred to initiate extradition proceedings for the return of the person;

(*d*) The person transferred shall receive credit for service of the sentence being served in the State from which he or she was transferred for time spent in the custody of the State Party to which he or she was transferred.

12. Unless the State Party from which a person is to be transferred in accordance with paragraphs 10 and 11 of this article so agrees, that person, whatever his or her nationality, shall not be prosecuted, detained, punished or subjected to any other restriction of his or her personal liberty in the territory of the State to which that person is transferred in respect of acts, omissions or convictions prior to his or her departure from the territory of the State from which he or she was transferred.

13. Each State Party shall designate a central authority that shall have the responsibility and power to receive requests for mutual legal assistance and either to execute them or to transmit them to the competent authorities for execution. Where a State Party has a special region or territory with a separate system of mutual legal assistance, it may designate a distinct central authority that shall have the same function for that region or territory. Central authorities shall ensure the speedy and proper execution or transmission of the requests received. Where the central authority transmits the request to a competent authority for execution, it shall encourage the speedy and proper execution of the request by the competent authority. The Secretary-General of the United Nations shall be notified of the central authority designated for this purpose at the time each State Party deposits its instrument of ratification, acceptance or approval of or accession to this Convention. Requests for mutual legal assistance and any communication related thereto shall be transmitted to the central authorities designated by the States Parties. This requirement shall be without prejudice to the right of a State Party to require that such requests and communications be addressed to it through diplomatic channels and, in urgent circumstances, where the States Parties agree, through the International Criminal Police Organization, if possible.

14. Requests shall be made in writing or, where possible, by any means capable of producing a written record, in a language acceptable to the requested State Party, under conditions allowing that State Party to establish authenticity. The Secretary-General of the United Nations shall be notified of the language or languages acceptable to each State Party at the time it deposits its instrument of ratification, acceptance or approval of or accession to this Convention. In urgent circumstances and where agreed by the States Parties, requests may be made orally, but shall be confirmed in writing forthwith.

15. A request for mutual legal assistance shall contain:

(*a*) The identity of the authority making the request;

(*b*) The subject matter and nature of the investigation, prosecution or judicial proceeding to which the request relates and the name and functions of the authority conducting the investigation, prosecution or judicial proceeding;

(*c*) A summary of the relevant facts, except in relation to requests for the purpose of service of judicial documents;

(*d*) A description of the assistance sought and details of any particular procedure that the requesting State Party wishes to be followed;

(*e*) Where possible, the identity, location and nationality of any person concerned; and

(*f*) The purpose for which the evidence, information or action is sought.

16. The requested State Party may request additional information when it appears necessary for the execution of the request in accordance with its domestic law or when it can facilitate such execution.

17. A request shall be executed in accordance with the domestic law of the requested State Party and, to the extent not contrary to the domestic law of the requested State Party and where possible, in accordance with the procedures specified in the request.

18. Wherever possible and consistent with fundamental principles of domestic law, when an individual is in the territory of a State Party and has to be heard as a witness or expert by the judicial authorities of another State Party, the first State Party may, at the request of the other, permit the hearing to take place by video conference if it is not possible or desirable for the individual in question to appear in person in the territory of the requesting State Party. States Parties may agree that the hearing shall be conducted by a judicial authority of the requesting State Party and attended by a judicial authority of the requested State Party.

19. The requesting State Party shall not transmit or use information or evidence furnished by the requested State Party for investigations, prosecutions or judicial proceedings other than those stated in the request without the prior consent of the requested State Party. Nothing in this paragraph shall prevent the requesting State Party from disclosing in its proceedings information or evidence that is exculpatory to an accused person. In the latter case, the requesting State Party shall notify the requested State Party prior to the disclosure and, if so requested, consult with the requested State Party. If, in an exceptional case, advance notice is not possible, the requesting State Party shall inform the requested State Party of the disclosure without delay.

20. The requesting State Party may require that the requested State Party keep confidential the fact and substance of the request, except to the extent necessary to execute the request. If the requested State Party cannot comply with the requirement of confidentiality, it shall promptly inform the requesting State Party.

21. Mutual legal assistance may be refused:

(*a*) If the request is not made in conformity with the provisions of this article;

(*b*) If the requested State Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests;

(*c*) If the authorities of the requested State Party would be prohibited by its domestic law from carrying out the action requested with regard to any similar offence, had it been subject to investigation, prosecution or judicial proceedings under their own jurisdiction;

(*d*) If it would be contrary to the legal system of the requested State Party relating to mutual legal assistance for the request to be granted.

22. States Parties may not refuse a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters.

23. Reasons shall be given for any refusal of mutual legal assistance.

24. The requested State Party shall execute the request for mutual legal assistance as soon as possible and shall take as full account as possible of any deadlines suggested by the requesting State Party and for which reasons are given, preferably in the request. The requested State Party shall respond to reasonable requests by the requesting State Party on progress of its handling of the request. The requesting State

Party shall promptly inform the requested State Party when the assistance sought is no longer required.

25. Mutual legal assistance may be postponed by the requested State Party on the ground that it interferes with an ongoing investigation, prosecution or judicial proceeding.

26. Before refusing a request pursuant to paragraph 21 of this article or postponing its execution pursuant to paragraph 25 of this article, the requested State Party shall consult with the requesting State Party to consider whether assistance may be granted subject to such terms and conditions as it deems necessary. If the requesting State Party accepts assistance subject to those conditions, it shall comply with the conditions.

27. Without prejudice to the application of paragraph 12 of this article, a witness, expert or other person who, at the request of the requesting State Party, consents to give evidence in a proceeding or to assist in an investigation, prosecution or judicial proceeding in the territory of the requesting State Party shall not be prosecuted, detained, punished or subjected to any other restriction of his or her personal liberty in that territory in respect of acts, omissions or convictions prior to his or her departure from the territory of the requested State Party. Such safe conduct shall cease when the witness, expert or other person having had, for a period of fifteen consecutive days or for any period agreed upon by the States Parties from the date on which he or she has been officially informed that his or her presence is no longer required by the judicial authorities, an opportunity of leaving, has nevertheless remained voluntarily in the territory of the requesting State Party or, having left it, has returned of his or her own free will.

28. The ordinary costs of executing a request shall be borne by the requested State Party, unless otherwise agreed by the States Parties concerned. If expenses of a substantial or extraordinary nature are or will be required to fulfil the request, the States Parties shall consult to determine the terms and conditions under which the request will be executed, as well as the manner in which the costs shall be borne.

29. The requested State Party:

(*a*) Shall provide to the requesting State Party copies of government records, documents or information in its possession that under its domestic law are available to the general public;

(*b*) May, at its discretion, provide to the requesting State Party in whole, in part or subject to such conditions as it deems appropriate, copies of any government records, documents or information in its possession that under its domestic law are not available to the general public.

30. States Parties shall consider, as may be necessary, the possibility of concluding bilateral or multilateral agreements or arrangements that would serve the purposes of, give practical effect to or enhance the provisions of this article.

Article 46 UNCAC. Mutual Legal Assistance

1. States Parties shall afford one another the widest measure of mutual legal assistance in investigations, prosecutions and judicial proceedings in relation to the offences covered by this Convention.

2. Mutual legal assistance shall be afforded to the fullest extent possible under relevant laws, treaties, agreements and arrangements of the requested State Party with respect to investigations, prosecutions and judicial proceedings in relation to the offences for which a legal person may be held liable in accordance with article 26 of this Convention in the requesting State Party.

3. Mutual legal assistance to be afforded in accordance with this article may be requested for any of the following purposes:

(*a*) Taking evidence or statements from persons;

(*b*) Effecting service of judicial documents;

(*c*) Executing searches and seizures, and freezing;

(*d*) Examining objects and sites;

(*e*) Providing information, evidentiary items and expert evaluations;

(*f*) Providing originals or certified copies of relevant documents and records, including government, bank, financial, corporate or business records;

(*g*) Identifying or tracing proceeds of crime, property, instrumentalities or other things for evidentiary purposes;

(*h*) Facilitating the voluntary appearance of persons in the requesting State Party;

(*i*) Any other type of assistance that is not contrary to the domestic law of the requested State Party;

(*j*) Identifying, freezing and tracing proceeds of crime in accordance with the provisions of chapter V of this Convention;

(*k*) The recovery of assets, in accordance with the provisions of chapter V of this Convention.

4. Without prejudice to domestic law, the competent authorities of a State Party may, without prior request, transmit information relating to criminal matters to a competent authority in another State Party where they believe that such information could assist the authority in undertaking or successfully concluding inquiries and criminal proceedings or could result in a request formulated by the latter State Party pursuant to this Convention.

5. The transmission of information pursuant to paragraph 4 of this article shall be without prejudice to inquiries and criminal proceedings in the State of the competent authorities providing the information. The competent authorities receiving the information shall comply with a request that said information remain confidential, even temporarily, or with restrictions on its use. However, this shall not prevent the receiving State Party from disclosing in its proceedings information that is exculpatory to an accused person. In such a case, the receiving State Party shall notify the transmitting State Party prior to the disclosure and, if so requested, consult with the transmitting State Party. If, in an exceptional case, advance notice is not possible, the receiving State Party shall inform the transmitting State Party of the disclosure without delay.

6. The provisions of this article shall not affect the obligations under any other treaty, bilateral or multilateral, that governs or will govern, in whole or in part, mutual legal assistance.

7. Paragraphs 9 to 29 of this article shall apply to requests made pursuant to this article if the States Parties in question are not bound by a treaty of mutual legal assistance. If those States Parties are bound by such a treaty, the corresponding provisions of that treaty shall apply unless the States Parties agree to apply paragraphs 9 to 29 of this article in lieu thereof. States Parties are strongly encouraged to apply those paragraphs if they facilitate cooperation.

8. States Parties shall not decline to render mutual legal assistance pursuant to this article on the ground of bank secrecy.

9. (*a*) A requested State Party, in responding to a request for assistance pursuant to this article in the absence of dual criminality, shall take into account the purposes of this Convention, as set forth in article 1;

(*b*) States Parties may decline to render assistance pursuant to this article on the ground of absence of dual criminality. However, a requested State Party shall, where consistent with the basic concepts of its legal system, render assistance that does not involve coercive action. Such assistance may be refused when requests

involve matters of a de minimis nature or matters for which the cooperation or assistance sought is available under other provisions of this Convention;

(*c*) Each State Party may consider adopting such measures as may be necessary to enable it to provide a wider scope of assistance pursuant to this article in the absence of dual criminality.

10. A person who is being detained or is serving a sentence in the territory of one State Party whose presence in another State Party is requested for purposes of identification, testimony or otherwise providing assistance in obtaining evidence for investigations, prosecutions or judicial proceedings in relation to offences covered by this Convention may be transferred if the following conditions are met:

(*a*) The person freely gives his or her informed consent;

(*b*) The competent authorities of both States Parties agree, subject to such conditions as those States Parties may deem appropriate.

11. For the purposes of paragraph 10 of this article:

(*a*) The State Party to which the person is transferred shall have the authority and obligation to keep the person transferred in custody, unless otherwise requested or authorized by the State Party from which the person was transferred;

(*b*) The State Party to which the person is transferred shall without delay implement its obligation to return the person to the custody of the State Party from which the person was transferred as agreed beforehand, or as otherwise agreed, by the competent authorities of both States Parties;

(*c*) The State Party to which the person is transferred shall not require the State Party from which the person was transferred to initiate extradition proceedings for the return of the person;

(*d*) The person transferred shall receive credit for service of the sentence being served in the State from which he or she was transferred for time spent in the custody of the State Party to which he or she was transferred.

12. Unless the State Party from which a person is to be transferred in accordance with paragraphs 10 and 11 of this article so agrees, that person, whatever his or her nationality, shall not be prosecuted, detained, punished or subjected to any other restriction of his or her personal liberty in the territory of the State to which that person is transferred in respect of acts, omissions or convictions prior to his or her departure from the territory of the State from which he or she was transferred.

13. Each State Party shall designate a central authority that shall have the responsibility and power to receive requests for mutual legal assistance and either to execute them or to transmit them to the competent authorities for execution. Where a State Party has a special region or territory with a separate system of mutual legal assistance, it may designate a distinct central authority that shall have the same function for that region or territory. Central authorities shall ensure the speedy and proper execution or transmission of the requests received. Where the central authority transmits the request to a competent authority for execution, it shall encourage the speedy and proper execution of the request by the competent authority. The Secretary-General of the United Nations shall be notified of the central authority designated for this purpose at the time each State Party deposits its instrument of ratification, acceptance or approval of or accession to this Convention. Requests for mutual legal assistance and any communication related thereto shall be transmitted to the central authorities designated by the States Parties. This requirement shall be without prejudice to the right of a State Party to require that such requests and communications be addressed to it through diplomatic channels and, in urgent circumstances, where the States Parties agree, through the International Criminal Police Organization, if possible.

14. Requests shall be made in writing or, where possible, by any means capable of producing a written record, in a language acceptable to the requested State Party,

under conditions allowing that State Party to establish authenticity. The Secretary-General of the United Nations shall be notified of the language or languages acceptable to each State Party at the time it deposits its instrument of ratification, acceptance or approval of or accession to this Convention. In urgent circumstances and where agreed by the States Parties, requests may be made orally but shall be confirmed in writing forthwith.

15. A request for mutual legal assistance shall contain:

(*a*) The identity of the authority making the request;

(*b*) The subject matter and nature of the investigation, prosecution or judicial proceeding to which the request relates and the name and functions of the authority conducting the investigation, prosecution or judicial proceeding;

(*c*) A summary of the relevant facts, except in relation to requests for the purpose of service of judicial documents;

(*d*) A description of the assistance sought and details of any particular procedure that the requesting State Party wishes to be followed;

(*e*) Where possible, the identity, location and nationality of any person concerned; and

(*f*) The purpose for which the evidence, information or action is sought.

16. The requested State Party may request additional information when it appears necessary for the execution of the request in accordance with its domestic law or when it can facilitate such execution.

17. A request shall be executed in accordance with the domestic law of the requested State Party and, to the extent not contrary to the domestic law of the requested State Party and where possible, in accordance with the procedures specified in the request.

18. Wherever possible and consistent with fundamental principles of domestic law, when an individual is in the territory of a State Party and has to be heard as a witness or expert by the judicial authorities of another State Party, the first State Party may, at the request of the other, permit the hearing to take place by video conference if it is not possible or desirable for the individual in question to appear in person in the territory of the requesting State Party. States Parties may agree that the hearing shall be conducted by a judicial authority of the requesting State Party and attended by a judicial authority of the requested State Party.

19. The requesting State Party shall not transmit or use information or evidence furnished by the requested State Party for investigations, prosecutions or judicial proceedings other than those stated in the request without the prior consent of the requested State Party. Nothing in this paragraph shall prevent the requesting State Party from disclosing in its proceedings information or evidence that is exculpatory to an accused person. In the latter case, the requesting State Party shall notify the requested State Party prior to the disclosure and, if so requested, consult with the requested State Party. If, in an exceptional case, advance notice is not possible, the requesting State Party shall inform the requested State Party of the disclosure without delay.

20. The requesting State Party may require that the requested State Party keep confidential the fact and substance of the request, except to the extent necessary to execute the request. If the requested State Party cannot comply with the requirement of confidentiality, it shall promptly inform the requesting State Party.

21. Mutual legal assistance may be refused:

(*a*) If the request is not made in conformity with the provisions of this article;

(*b*) If the requested State Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests;

(*c*) If the authorities of the requested State Party would be prohibited by its domestic law from carrying out the action requested with regard to any similar offence, had it been subject to investigation, prosecution or judicial proceedings under their own jurisdiction;

(*d*) If it would be contrary to the legal system of the requested State Party relating to mutual legal assistance for the request to be granted.

22. States Parties may not refuse a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters.

23. Reasons shall be given for any refusal of mutual legal assistance.

24. The requested State Party shall execute the request for mutual legal assistance as soon as possible and shall take as full account as possible of any deadlines suggested by the requesting State Party and for which reasons are given, preferably in the request. The requesting State Party may make reasonable requests for information on the status and progress of measures taken by the requested State Party to satisfy its request. The requested State Party shall respond to reasonable requests by the requesting State Party on the status, and progress in its handling, of the request. The requesting State Party shall promptly inform the requested State Party when the assistance sought is no longer required.

25. Mutual legal assistance may be postponed by the requested State Party on the ground that it interferes with an ongoing investigation, prosecution or judicial proceeding.

26. Before refusing a request pursuant to paragraph 21 of this article or postponing its execution pursuant to paragraph 25 of this article, the requested State Party shall consult with the requesting State Party to consider whether assistance may be granted subject to such terms and conditions as it deems necessary. If the requesting State Party accepts assistance subject to those conditions, it shall comply with the conditions.

27. Without prejudice to the application of paragraph 12 of this article, a witness, expert or other person who, at the request of the requesting State Party, consents to give evidence in a proceeding or to assist in an investigation, prosecution or judicial proceeding in the territory of the requesting State Party shall not be prosecuted, detained, punished or subjected to any other restriction of his or her personal liberty in that territory in respect of acts, omissions or convictions prior to his or her departure from the territory of the requested State Party. Such safe conduct shall cease when the witness, expert or other person having had, for a period of fifteen consecutive days or for any period agreed upon by the States Parties from the date on which he or she has been officially informed that his or her presence is no longer required by the judicial authorities, an opportunity of leaving, has nevertheless remained voluntarily in the territory of the requesting State Party or, having left it, has returned of his or her own free will.

28. The ordinary costs of executing a request shall be borne by the requested State Party, unless otherwise agreed by the States Parties concerned. If expenses of a substantial or extraordinary nature are or will be required to fulfil the request, the States Parties shall consult to determine the terms and conditions under which the request will be executed, as well as the manner in which the costs shall be borne.

29. The requested State Party:

(*a*) Shall provide to the requesting State Party copies of government records, documents or information in its possession that under its domestic law are available to the general public;

(*b*) May, at its discretion, provide to the requesting State Party in whole, in part or subject to such conditions as it deems appropriate, copies of any government records, documents or information in its possession that under its domestic law are not available to the general public.

30. States Parties shall consider, as may be necessary, the possibility of concluding bilateral or multilateral agreements or arrangements that would serve the purposes of, give practical effect to or enhance the provisions of this article.

Article 25 Budapest Convention. General Principles Relating to Mutual Assistance

1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2. Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or email, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4. Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 32 League of Arab States Convention. Mutual Assistance

1. All State Party shall lend assistance to each other to the fullest extent for the purposes of investigation, procedures related to information and information technology offences or to gather electronic evidence in offences.

2. Every State Party shall commit itself to adopting the procedures necessary to fulfil the obligations set forth in Articles 34 to 42.

3. Requests for bilateral assistance and related communications shall be submitted in writing. In case of emergency, a State Party may submit such request in an expeditious manner, including by fax or email, provided such communication ensures a reasonable degree of security and reference (including by using coding) and confirmation of dispatch as required by the State Party. The State Party from which assistance is requested shall respond to the request through a fast means of communication.

4. Except as otherwise stated in this chapter, bilateral assistance shall be subject to the requirements set forth in the law of the State Party from which assistance is requested or in mutual assistance treaties, including the grounds on which the State Party can rely to refuse cooperation. The State Party from which assistance is requested may not exercise its right to refuse assistance with respect to offenses set forth in Chapter II only on the basis that the request relates to an offence that it considers as a financial offence.

5. Whenever the State Party from which assistance is requested may provide such assistance only in the presence of dual criminality, this condition shall be considered

fulfilled regardless of whether the laws of the State Party classify the offence in the same category as those of the requesting State Party, provided that the act leading to the offence in respect of which assistance is requested is considered an offence according to the laws of the State Party.

Article 34 League of Arab States Convention. Procedures for Cooperation and Mutual Assistance Requests

1. The provisions of paragraphs 2-9 of this Article shall apply in case no cooperation and mutual assistance treaty or convention exists on the basis of the applicable legislation between the State Parties requesting assistance and those from which assistance is requested. If such a treaty or convention exists, the mentioned paragraphs shall not apply, unless the concerned parties agree to apply them in full or in part.

2. (*a*) Every State Party shall designate a central authority responsible for sending and responding to mutual assistance requests and for their implementation and referral to the relevant authorities for implementation.

(*b*) Central authorities shall communicate directly among themselves.

(*c*) Every State Party shall, at the time of signature or deposit of the instrument of ratification, acceptance or agreement, contact the General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers and communicate to them the names and addresses of the authorities specifically designated for the purposes of this paragraph.

(*d*) The General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers shall establish and update a registry of concerned central authorities appointed by the State Parties. Every State Party shall insure that the registry's details are correct at all times.

3. Mutual assistance requests in this Article shall be implemented according to procedures specified by the requesting State Party, except in the case of non-conformity with the law of the State Party from which assistance is requested.

4. The State Party from which assistance is requested may postpone taking action on the request if such action shall affect criminal investigations conducted by its authorities.

5. Prior to refusing or postponing assistance, the State Party from which assistance is requested shall decide, after consulting with the requesting State Party, whether the request shall be partially fulfilled or be subject to whatever conditions it may deem necessary.

6. The State Party from which assistance is requested shall commit itself to inform the requesting State Party of the result of the implementation of the request. If the request is refused or postponed, the reasons of such refusal or postponement shall be given. The State Party from which assistance is requested shall inform the requesting State Party of the reasons that prevent the complete fulfilment of the request or the reasons for its considerable postponement.

7. The State Party requesting assistance may request the State Party from which assistance is requested to maintain the confidentiality of the nature and content of any request covered by this chapter, except in as far as necessary to implement the request. If the State Party from which assistance is requested cannot abide by this request concerning confidentiality, it shall so inform the requesting State Party which will then decide about the possibility of implementing the request.

8. (*a*) In case of emergency, mutual assistance requests may be sent directly to the judicial authorities in the State Party from which assistance is requested from their counterparts in the requesting State Party. In such case, a copy shall be sent concurrently from the central authority in the requesting State Party to its counterpart in the State Party from which assistance is requested.

(*b*) Communications can be made and requests submitted pursuant to this paragraph through INTERPOL.

(*c*) Whenever, according to paragraph a, a request is submitted to an authority, but that authority is not competent to deal with that request, it shall refer the request to the competent authority and directly inform the requesting State Party accordingly.

(*d*) Communications and requests carried out according to this paragraph and not concerning compulsory procedures may be transmitted directly by the competent authorities in the requesting State Party to their counterpart in the State Party from which assistance is requested.

(*e*) Every State Party may, at the time of signature, ratification, acceptance or adoption, inform the General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers that requests according to this paragraph must be submitted to the central authority for reasons of efficiency.

Article 6 Dushanbe Agreement. Request for Assistance

1. Cooperation under this Agreement shall be carried out on the basis of requests for assistance from the competent authorities of the Parties (hereinafter referred to as the request). The information may be provided to the competent authority of another Party without request, if there is reason to believe that it is of interest to the said competent authority.

2. The request shall be made in writing. In urgent cases, requests may be transmitted using technical means of communication or orally, but must then be confirmed in writing within 3 days. The request and materials of the executed request may be transmitted via technical channels of communication if there is a bilateral agreement between the competent authorities of the Parties or if these channels are defined by other international treaties to which the Parties are parties.

3. The request must contain:

(*a*) the name of the competent authority of the requesting Party and the competent authority of the requested Party;

(*b*) a statement of the facts of the case;

(*c*) an indication of the purpose and justification for the request;

(*d*) the content of the requested assistance;

(*e*) the desired time frame for the execution of the request;

(*f*) any other information that may be helpful in executing the request, including relevant documents or certified copies thereof;

(*g*) a reference to this Agreement.

4. A request transmitted or acknowledged in writing shall be signed by:

(*a*) the head or deputy head of the requesting competent authority and affixed with the stamp of the competent authority, if the information is exchanged between non-core units of competent authorities;

(*b*) the head of an independent central specialized subdivision of the competent authority and shall be sealed with the stamp of the independent central specialized subdivision of the competent authority – if the exchange of information is carried out between the independent specialized subdivisions of the competent authorities.

Article 7 Dushanbe Agreement. Execution of the Request

1. The competent authority of the requested Party shall take all measures necessary to ensure the complete and quality execution of the request within the time limit indicated by the competent authority of the requesting Party.

2. The competent authority of the requesting Party shall be informed without delay of the circumstances preventing or significantly delaying the execution of the request.

3. If the execution of the request is not within the competence of the competent authority of the requested Party, the said competent authority shall forthwith transmit it to the appropriate competent authority of the requested Party and shall inform the initiator of the request accordingly.

4. In executing the request, the law of the requested Party shall apply.

5. The competent authority of the requested Party may, at the request of the competent authority of the requesting Party, allow its representatives to be present when the request is executed.

6. If the competent authority of the requested Party considers that the execution of the request may interfere with prosecutions or other proceedings pending in the territory of the requested Party, it may postpone the execution of the request or subject its execution to conditions specified as necessary, after consulting with the competent authority of the requesting Party. If the competent authority of the requesting Party agrees to receive assistance subject to the conditions proposed, it shall comply with those conditions.

7. The competent authority of the requested Party shall, as soon as possible, inform the competent authority of the requesting Party of the results of the execution of the request.

Article 8 Dushanbe Agreement. Confidentiality of Information

1. The competent authorities of the Parties shall ensure the confidentiality of the information received pursuant to this Agreement, including the fact of receipt and the contents of the request, if the competent authority of the requesting Party considers it undesirable to disclose it.

2. If the request cannot be executed confidentially, the competent authority of the requested Party shall inform the competent authority of the requesting Party in order to decide whether the request can be executed under those conditions.

3. If the competent authority of the requesting Party does not agree to execute the request on those conditions, the competent authority of the requested Party shall be informed of the decision.

Article 9 Dushanbe Agreement. Use of Request Execution Results

1. The results of the execution of the request may not be used without the consent of the competent authority of the requested Party that provided them for purposes other than those for which they were requested and provided.

2. The competent authority of the requesting Party may use the results of the execution of the request for other purposes only with the written consent of the competent authority of the requested Party. In such cases, the competent authority of the requesting Party shall observe the restrictions on the use of the results of the request as established by the competent authority of the requested Party.

Article 10 Dushanbe Agreement. Transmission of Information to a Third Party

The transmission to a third party of information obtained by the competent authority of the requesting Party pursuant to this Agreement requires the prior written consent of the competent authority of the requested Party that provided the information.

Article 11 Dushanbe Agreement. Refusal to Execute a Request

1. The execution of a request under this Agreement may be refused in whole or in part if the competent authority of the requested Party considers that the execution of the request may prejudice the sovereignty, security or national interests of its State,

public order, as well as the rights and legitimate interests of citizens, contrary to the national law or international obligations of the requested Party.

2. In the event of a decision to refuse to execute a request, the competent authority of the requested Party shall, without delay, inform the competent authority of the requesting Party in writing of its decision.

6. Provision of unsolicited information/exchange of information

Article 18, paragraphs 4 and 5 UNTOC. Mutual Legal Assistance

4. Without prejudice to domestic law, the competent authorities of a State Party may, without prior request, transmit information relating to criminal matters to a competent authority in another State Party where they believe that such information could assist the authority in undertaking or successfully concluding inquiries and criminal proceedings or could result in a request formulated by the latter State Party pursuant to this Convention.

5. The transmission of information pursuant to paragraph 4 of this article shall be without prejudice to inquiries and criminal proceedings in the State of the competent authorities providing the information. The competent authorities receiving the information shall comply with a request that said information remain confidential, even temporarily, or with restrictions on its use. However, this shall not prevent the receiving State Party from disclosing in its proceedings information that is exculpatory to an accused person. In such a case, the receiving State Party shall notify the transmitting State Party prior to the disclosure and, if so requested, consult with the transmitting State Party. If, in an exceptional case, advance notice is not possible, the receiving State Party shall inform the transmitting State Party of the disclosure without delay.

Article 46, paragraphs 4 and 5 UNCAC. Mutual Legal Assistance

4. Without prejudice to domestic law, the competent authorities of a State Party may, without prior request, transmit information relating to criminal matters to a competent authority in another State Party where they believe that such information could assist the authority in undertaking or successfully concluding inquiries and criminal proceedings or could result in a request formulated by the latter State Party pursuant to this Convention.

5. The transmission of information pursuant to paragraph 4 of this article shall be without prejudice to inquiries and criminal proceedings in the State of the competent authorities providing the information. The competent authorities receiving the information shall comply with a request that said information remain confidential, even temporarily, or with restrictions on its use. However, this shall not prevent the receiving State Party from disclosing in its proceedings information that is exculpatory to an accused person. In such a case, the receiving State Party shall notify the transmitting State Party prior to the disclosure and, if so requested, consult with the transmitting State Party. If, in an exceptional case, advance notice is not possible, the receiving State Party shall inform the transmitting State Party of the disclosure without delay.

Article 26 Budapest Convention. Spontaneous Information

1. A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2. Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then

determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Article 33 League of Arab States Convention. Circumstantial Information

1. A State Party may – within the confines of its domestic law – and without prior request, give another State information it obtained through its investigations if it considers that the disclosure of such information could help the receiving State Party in investigating offences set forth in this convention or could lead to a request for cooperation from that State Party.

2. Before giving such information, the State Party providing it may request that the confidentiality of the information be kept; if the receiving State Party cannot abide by this request, it shall so inform the State Party providing the information which will then decide about the possibility of providing the information. If the receiving State Party accepts the information on condition of confidentiality, the information shall remain between the two sides.

7. Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27 Budapest Convention. Procedures Pertaining to Mutual Assistance Requests in the Absence of Applicable International Agreements

1. Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2. (*a*) Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

(*b*) The central authorities shall communicate directly with each other;

(*c*) Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

(*d*) The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3. Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4. The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

(*a*) the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

(*b*) it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5. The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6. Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7. The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8. The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9. (*a*) In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

(*b*) Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

(*c*) Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

(*d*) Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

(*e*) Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

8. Confidentiality and limitation on use

Article 28 Budapest Convention. Confidentiality and Limitation on Use

1. When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2. The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

(*a*) kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

(*b*) not used for investigations or proceedings other than those stated in the request.

3. If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4. Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Article 36 League of Arab States Convention. Confidentiality and Limits of Utilization

1. In case no mutual assistance treaty or agreement exists on the basis of the applicable legislation between the State Parties requesting assistance and those from which assistance is requested, the provisions of this Article shall apply. These provisions shall not apply if such a convention or treaty exists unless the concerned State Parties agree to apply any of the paragraphs of this Article or the whole Article.

2. The State Party from which assistance is requested may provide information or material contained in the request, provided:

(*a*) The element of confidentiality is maintained for the State Party requesting assistance; there shall be no compliance with the request in the absence of this element.

(*b*) The information is not used in investigations other than those contained in the request.

3. If the State Party requesting assistance cannot abide by the requirement set forth in paragraph 2, it shall so inform the other State Party which will then decide about the possibility of providing the information. If the requesting State Party accepts this requirement, it shall abide by it.

4. A State Party providing information or material according to the requirement in paragraph 2 concerning the provision of information may request the other State Party to justify the use of the information or material.

Article 6 SCO Agreement. Protection of Information

1. This Agreement shall not mandate the Parties to provide information in the framework of the cooperation under this Agreement and it shall not warrant transmitting information in the framework of this cooperation, if the disclosure of such information may harm national interests.

2. In the framework of cooperation under this Agreement, the Parties shall not exchange information regarded as a state secret according to the law of any of the Party. The procedure for the transferring and handling such information, which in specific cases may be considered necessary for the purposes of this Agreement, shall be based on the relevant agreements between the Parties and on the terms thereof.

3. The Parties shall ensure adequate protection of the information transmitted or generated in the course of cooperation under this Agreement provided that this information is not considered as state secret by the laws of any of the Parties, access and dissemination of which is limited in accordance with the law and/or the relevant regulations of any of the Party.

Such information shall be protected in accordance with the legislation and/or the relevant regulations of the receiving Party. Such information shall not be disclosed or transferred without the written consent of the Party that originated this information.

Such information shall be duly marked in accordance with the legislation and/or the relevant regulations of the Parties.

9. Mutual assistance regarding provisional measures

(a) Assistance – preservation of computer data/information

Article 29 Budapest Convention. Expedited Preservation of Stored Computer Data

1. A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2. A request for preservation made under paragraph 1 shall specify:

(*a*) the authority seeking the preservation;

(*b*) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

(*c*) the stored computer data to be preserved and its relationship to the offence;

(*d*) any available information identifying the custodian of the stored computer data or the location of the computer system;

(*e*) the necessity of the preservation; and

(*f*) that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3. Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4. A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5. In addition, a request for preservation may only be refused if:

(*a*) the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

(*b*) the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

6. Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7. Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Article 37 League of Arab States Convention. Expeditious Safeguarding of Information Stored on Information Systems

1. A State Party may request another State Party to obtain the expeditious safeguarding of information stored on an information technology located within its territory regarding matters about which the State Party requesting assistance is submitting a request for mutual assistance in order to investigate, seize secure and disclose information.

2. A safeguarding request according to paragraph 1 shall specify the following:

(*a*) the authority requesting the safeguarding.

(*b*) the offence that is the subject of the investigation and a summary of the facts.

(*c*) the information technology information to be safeguarded and its relation to the crime.

(*d*) any available information that determines the person responsible for the stored information or the location of the information technology.

(*e*) the reasons for the safeguarding request.

(*f*) the desire of the State Party submitting the request for bilateral assistance to investigate, access, seize, secure or disclose the stored information technology information.

3. When a State Party receives a request from another State Party, it shall take all appropriate actions to safeguard the specified information in an expeditious manner according to its domestic law. For the purpose of responding to the request, safeguarding shall not be conditional on the existence of dual criminality.

4. A State Party that stipulates the existence of dual criminality to respond to the assistance request may, except in cases of crimes set forth in Chapter II of this Convention, reserve its right to refuse the safeguarding request according to this Article if there is reason to believe that the dual criminality requirement shall not be fulfilled at the time of disclosure.

5. Additionally, a safeguarding request may be refused if:

1. the request relates to an offence that the State Party from which assistance is requested considers as a political offence.

2. the State Party from which assistance is requested considers that implementing the request could threaten its sovereignty, security, order or interests.

6. Whenever the State Party from which assistance is requested believes that safeguarding will not guarantee the future availability of information or will jeopardize the confidentiality of the investigations of the requesting State Party or their integrity, it shall inform the requesting State Party accordingly so that it may subsequently determine the possibility of implementing the request.

7. A safeguarding that results from a response to the request mentioned in paragraph 1 shall be for a period of no less than 60 days in order to allow the requesting State Party to submit the request for searching, accessing, seizing, securing or disclosing information. After receipt of such a request, safeguarding of information shall be maintained according to the decision related to the request.

(b) Assistance – Seizure/access to/collection of/disclosure of computer data/information

Article 30 Budapest Convention. Expedited Disclosure of Preserved Traffic Data

1. Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2. Disclosure of traffic data under paragraph 1 may only be withheld if:

(*a*) the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

(*b*) the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

Article 31 Budapest Convention. Mutual Assistance Regarding Accessing of Stored Computer Data

1. A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located

within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2. The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

3. The request shall be responded to on an expedited basis where:

(*a*) there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

(*b*) the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 34 Budapest Convention. Mutual Assistance Regarding the Interception of Content Data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Article 38 League of Arab States Convention. Expeditious Disclosure of Safeguarded Users Tracking Information

1. Whenever the State Party from which assistance is requested determines – in the context of implementing, according to Article 37, a request to safeguard users tracking information related to specific communications – that a service provider in another state has participated in the transmission of the communication, the State Party from which assistance is requested shall disclose to the State Party requesting assistance a sufficient amount of users tracking information in order to determine the service provider and the transmission path of the communications.

2. The disclosure of users tracking information according to paragraph 1 may be suspended if:

1. the request relates to an offence that the State Party from which assistance is requested considers as a political offence.

2. the State Party from which assistance is requested considers that implementing the request could threaten its safety, security, order or interests

Article 39 League of Arab States Convention. Cooperation and Bilateral Assistance Regarding Access to Stored Information Technology Information

1. A State Party may request another State Party to investigate, access, seize, secure or disclose the stored information technology information located within the territory of the State Party from which assistance is requested, including information that has been safeguarded according to Article 37.

2. The State Party from which assistance is requested shall commit itself to respond to the State Party requesting assistance according to the provisions of this convention.

3. The response to the request shall be prompt if the relevant information may be lost or amended.

Article 41 League of Arab States Convention. Cooperation and Bilateral Assistance Regarding the Expeditious Gathering of Users Tracking Information

1. State Parties shall lend bilateral assistance to each other regarding the expeditious gathering of users tracking information associated with specific communications in their territories and transmitted through the information technology.

2. Every State Party shall provide such assistance at least with respect to offences for which similar domestic cases involve the expeditious gathering of users tracking information.

Article 42 League of Arab States Convention. Cooperation and Bilateral Assistance Regarding Information Related to Content

State Parties shall commit themselves to provide bilateral assistance to each other regarding the expeditious gathering of content information for specific communications transmitted by means of the information technology up to the limit allowed according to applicable treaties and local laws.

10. Trans-border access to computer data/information

Article 32 Budapest Convention. Trans-Border Access to Stored Computer Data with Consent or Where Publicly Available

A Party may, without the authorisation of another Party:

(*a*) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

(*b*) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 40 League of Arab States Convention. Access to Information Technology Information Across Borders

A State Party may, without obtaining an authorization from another State Party:

1. Access information technology information available to the public (open source), regardless of the geographical location of the information.

2. Access or receive – through information technology in its territory – information technology information found in the other State Party, provided it has obtained the voluntary and legal agreement of the person having the legal authority to disclose information to that State Party by means of the said information technology.

11. Mutual assistance regarding the real-time collection of traffic data

Article 33 Budapest Convention. Mutual Assistance Regarding the Real-Time Collection of Traffic Data

1. The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2. Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

12. Dual criminality

Article 24(1) Budapest Convention. Extradition

1. (*a*) This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

(*b*) Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty,

including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

Article 25(5) Budapest Convention. General Principles Relating to Mutual Assistance

5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 32(5) League of Arab States Convention. Mutual Assistance

5. Whenever the State Party from which assistance is requested may provide such assistance only in the presence of dual criminality, this condition shall be considered fulfilled regardless of whether the laws of the State Party classify the offence in the same category as those of the requesting State Party, provided that the act leading to the offence in respect of which assistance is requested is considered an offence according to the laws of the State Party.

Article 37(3)(4) League of Arab States Convention. Expeditious Safeguarding of Information Stored on Information Systems

3. When a State Party receives a request from another State Party, it shall take all appropriate actions to safeguard the specified information in an expeditious manner according to its domestic law. For the purpose of responding to the request, safeguarding shall not be conditional on the existence of dual criminality.

4. A State Party that stipulates the existence of dual criminality to respond to the assistance request may, except in cases of crimes set forth in Chapter II of this Convention, reserve its right to refuse the safeguarding request according to this Article if there is reason to believe that the dual criminality requirement shall not be fulfilled at the time of disclosure.

13. Law enforcement cooperation

Article 27 UNTOC. Law Enforcement Cooperation

1. States Parties shall cooperate closely with one another, consistent with their respective domestic legal and administrative systems, to enhance the effectiveness of law enforcement action to combat the offences covered by this Convention. Each State Party shall, in particular, adopt effective measures:

(*a*) To enhance and, where necessary, to establish channels of communication between their competent authorities, agencies and services in order to facilitate the secure and rapid exchange of information concerning all aspects of the offences covered by this Convention, including, if the States Parties concerned deem it appropriate, links with other criminal activities;

(*b*) To cooperate with other States Parties in conducting inquiries with respect to offences covered by this Convention concerning:

(*i*) The identity, whereabouts and activities of persons suspected of involvement in such offences or the location of other persons concerned;

(*ii*) The movement of proceeds of crime or property derived from the commission of such offences;

(*iii*) The movement of property, equipment or other instrumentalities used or intended for use in the commission of such offences;

(*c*) To provide, when appropriate, necessary items or quantities of substances for analytical or investigative purposes;

(*d*) To facilitate effective coordination between their competent authorities, agencies and services and to promote the exchange of personnel and other experts, including, subject to bilateral agreements or arrangements between the States Parties concerned, the posting of liaison officers;

(*e*) To exchange information with other States Parties on specific means and methods used by organized criminal groups, including, where applicable, routes and conveyances and the use of false identities, altered or false documents or other means of concealing their activities;

(*f*) To exchange information and coordinate administrative and other measures taken as appropriate for the purpose of early identification of the offences covered by this Convention.

2. With a view to giving effect to this Convention, States Parties shall consider entering into bilateral or multilateral agreements or arrangements on direct cooperation between their law enforcement agencies and, where such agreements or arrangements already exist, amending them. In the absence of such agreements or arrangements between the States Parties concerned, the Parties may consider this Convention as the basis for mutual law enforcement cooperation in respect of the offences covered by this Convention. Whenever appropriate, States Parties shall make full use of agreements or arrangements, including international or regional organizations, to enhance the cooperation between their law enforcement agencies.

3. States Parties shall endeavour to cooperate within their means to respond to transnational organized crime committed through the use of modern technology.

Article 48 UNCAC. Law Enforcement Cooperation

1. States Parties shall cooperate closely with one another, consistent with their respective domestic legal and administrative systems, to enhance the effectiveness of law enforcement action to combat the offences covered by this Convention. States Parties shall, in particular, take effective measures:

(*a*) To enhance and, where necessary, to establish channels of communication between their competent authorities, agencies and services in order to facilitate the secure and rapid exchange of information concerning all aspects of the offences covered by this Convention, including, if the States Parties concerned deem it appropriate, links with other criminal activities;

(*b*) To cooperate with other States Parties in conducting inquiries with respect to offences covered by this Convention concerning:

(*i*) The identity, whereabouts and activities of persons suspected of involvement in such offences or the location of other persons concerned;

(*ii*) The movement of proceeds of crime or property derived from the commission of such offences;

(*iii*) The movement of property, equipment or other instrumentalities used or intended for use in the commission of such offences;

(*c*) To provide, where appropriate, necessary items or quantities of substances for analytical or investigative purposes;

(*d*) To exchange, where appropriate, information with other States Parties concerning specific means and methods used to commit offences covered by this Convention, including the use of false identities, forged, altered or false documents and other means of concealing activities;

(*e*) To facilitate effective coordination between their competent authorities, agencies and services and to promote the exchange of personnel and other experts,

including, subject to bilateral agreements or arrangements between the States Parties concerned, the posting of liaison officers;

(*f*) To exchange information and coordinate administrative and other measures taken as appropriate for the purpose of early identification of the offences covered by this Convention.

2. With a view to giving effect to this Convention, States Parties shall consider entering into bilateral or multilateral agreements or arrangements on direct cooperation between their law enforcement agencies and, where such agreements or arrangements already exist, amending them. In the absence of such agreements or arrangements between the States Parties concerned, the States Parties may consider this Convention to be the basis for mutual law enforcement cooperation in respect of the offences covered by this Convention. Whenever appropriate, States Parties shall make full use of agreements or arrangements, including international or regional organizations, to enhance the cooperation between their law enforcement agencies.

3. States Parties shall endeavour to cooperate within their means to respond to offences covered by this Convention committed through the use of modern technology.

14. Joint investigations

Paragraph 27 IEG Recommendations

States are encouraged to establish joint investigative teams with other countries at the bilateral, regional or international levels to enhance enforcement capabilities.

Article 19 UNTOC. Joint Investigations

States Parties shall consider concluding bilateral or multilateral agreements or arrangements whereby, in relation to matters that are the subject of investigations, prosecutions or judicial proceedings in one or more States, the competent authorities concerned may establish joint investigative bodies. In the absence of such agreements or arrangements, joint investigations may be undertaken by agreement on a case-by-case basis. The States Parties involved shall ensure that the sovereignty of the State Party in whose territory such investigation is to take place is fully respected.

Article 49 UNCAC. Joint Investigations

States Parties shall consider concluding bilateral or multilateral agreements or arrangements whereby, in relation to matters that are the subject of investigations, prosecutions or judicial proceedings in one or more States, the competent authorities concerned may establish joint investigative bodies. In the absence of such agreements or arrangements, joint investigations may be undertaken by agreement on a case-by-case basis. The States Parties involved shall ensure that the sovereignty of the State Party in whose territory such investigation is to take place is fully respected.

15. Special investigative techniques

Article 20 UNTOC. Special Investigative Techniques

1. If permitted by the basic principles of its domestic legal system, each State Party shall, within its possibilities and under the conditions prescribed by its domestic law, take the necessary measures to allow for the appropriate use of controlled delivery and, where it deems appropriate, for the use of other special investigative techniques, such as electronic or other forms of surveillance and undercover operations, by its competent authorities in its territory for the purpose of effectively combating organized crime.

2. For the purpose of investigating the offences covered by this Convention, States Parties are encouraged to conclude, when necessary, appropriate bilateral or multilateral agreements or arrangements for using such special investigative techniques in the context of cooperation at the international level. Such agreements

or arrangements shall be concluded and implemented in full compliance with the principle of sovereign equality of States and shall be carried out strictly in accordance with the terms of those agreements or arrangements.

3. In the absence of an agreement or arrangement as set forth in paragraph 2 of this article, decisions to use such special investigative techniques at the international level shall be made on a case-by-case basis and may, when necessary, take into consideration financial arrangements and understandings with respect to the exercise of jurisdiction by the States Parties concerned.

4. Decisions to use controlled delivery at the international level may, with the consent of the States Parties concerned, include methods such as intercepting and allowing the goods to continue intact or be removed or replaced in whole or in part.

Article 50 UNCAC. Special Investigative Techniques

1. In order to combat corruption effectively, each State Party shall, to the extent permitted by the basic principles of its domestic legal system and in accordance with the conditions prescribed by its domestic law, take such measures as may be necessary, within its means, to allow for the appropriate use by its competent authorities of controlled delivery and, where it deems appropriate, other special investigative techniques, such as electronic or other forms of surveillance and undercover operations, within its territory, and to allow for the admissibility in court of evidence derived therefrom.

2. For the purpose of investigating the offences covered by this Convention, States Parties are encouraged to conclude, when necessary, appropriate bilateral or multilateral agreements or arrangements for using such special investigative techniques in the context of cooperation at the international level. Such agreements or arrangements shall be concluded and implemented in full compliance with the principle of sovereign equality of States and shall be carried out strictly in accordance with the terms of those agreements or arrangements.

3. In the absence of an agreement or arrangement as set forth in paragraph 2 of this article, decisions to use such special investigative techniques at the international level shall be made on a case-by-case basis and may, when necessary, take into consideration financial arrangements and understandings with respect to the exercise of jurisdiction by the States Parties concerned.

4. Decisions to use controlled delivery at the international level may, with the consent of the States Parties concerned, include methods such as intercepting and allowing the goods or funds to continue intact or be removed or replaced in whole or in part.

16. Transfer of Criminal Proceedings

Article 21 UNTOC. Transfer of Criminal Proceedings

States Parties shall consider the possibility of transferring to one another proceedings for the prosecution of an offence covered by this Convention in cases where such transfer is considered to be in the interests of the proper administration of justice, in particular in cases where several jurisdictions are involved, with a view to concentrating the prosecution.

Article 47 UNCAC. Transfer of Criminal Proceedings

States Parties shall consider the possibility of transferring to one another proceedings for the prosecution of an offence established in accordance with this Convention in cases where such transfer is considered to be in the interests of the proper administration of justice, in particular in cases where several jurisdictions are involved, with a view to concentrating the prosecution.

17. Exchange of information

Para. 13 IEG Recommendations

Member States are encouraged to increase their sharing of experiences and information, including national legislation, national procedures, best practices on cross-border cybercrime investigations, information on organized criminal groups and the techniques and methodology used by those groups.

Para. 24 IEG Recommendations

Member States should exchange information on how challenges in accessing digital evidence in a timely manner are being resolved domestically, in order for other Member States to benefit from those experiences and increase the efficiency and effectiveness of their own processes.

Article 28(2) UNTOC. Collection, Exchange, and Analysis of Information on the Nature of Organized Crime

2. States Parties shall consider developing and sharing analytical expertise concerning organized criminal activities with each other and through international and regional organizations. For that purpose, common definitions, standards and methodologies should be developed and applied as appropriate.

Article 61(2) UNCAC. Collection, Exchange and Analysis of Information on Corruption

2. States Parties shall consider developing and sharing with each other and through international and regional organizations statistics, analytical expertise concerning corruption and information with a view to developing, insofar as possible, common definitions, standards and methodologies, as well as information on best practices to prevent and combat corruption.

18. Exchange of information through CERTs

Article 28(3) AU Convention 2014. International Cooperation

3. Exchange of information

State Parties shall encourage the establishment of institutions that exchange information on cyber threats and vulnerability assessment such as the Computer Emergency Response Team (CERT) or the Computer Security Incident Response Team (CSIRTs).

19. Point of contact, 24/7 network, and other specialized networks

Paragraph 6 IEG Recommendations

Member States should explore ways to help to ensure that the exchange of information among investigators and prosecutors handling cybercrime is made in a timely and secure way, including by strengthening networks of national institutions that may be available 24/7.

Paragraph 23 IEG Recommendations

Countries are called upon to join, make wider use of and strengthen authorized networks of practitioners to preserve and exchange admissible electronic evidence, including 24/7 networks, specialized networks on cybercrime and International Criminal Police Organization (INTERPOL) channels for prompt police-to-police cooperation and other methods of informal cooperation before using mutual legal assistance channels was also recommended.

Article 35 Budapest Convention. 24/7 Network

1. Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

(*a*) the provision of technical advice;

(*b*) the preservation of data pursuant to Articles 29 and 30;

(*c*) the collection of evidence, the provision of legal information, and locating of suspects.

2. (*a*) A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

(*b*) If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3. Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Article 43 League of Arab States Convention. Specialized Body

1. Every State Party shall guarantee, according to the basic principles of its legal system, the presence of a specialized body dedicated 24 hours a day to ensure the provision of prompt assistance for the purposes of investigation, procedures related to information technology offences or gather evidence in electronic form regarding a specific offence. Such assistance shall involve facilitating or implementing:

(*a*) provision of technical advice.

(*b*) safeguarding information based on Articles 37 and 38.

(*c*) collecting evidence, provide legal information and locate suspects.

2. (*a*) In all State Parties, such a body shall be able to communicate promptly with the corresponding body in any other State party

(*b*) If the said body, designated by a State Party, is not part of the authorities of that State Party responsible for international bilateral assistance, that body shall ensure its ability to promptly coordinate with those authorities.

3. Every State Party shall ensure the availability of capable human resources to facilitate the work of the above mentioned body.

Article 5(1) SCO Agreement. Main Formats and Mechanisms of Cooperation

1. Within sixty days from the date of entry of this Agreement into force, the Parties, through the Depositary, shall exchange information about the competent authorities of the Parties responsible for the implementation of this Agreement, and the channels of direct exchange of information on specific areas of cooperation.

Article 4 Dushanbe Agreement. Competent Authorities

1. Cooperation of the Parties within the framework of this Agreement shall be carried out between the competent authorities directly.

2. The list of competent authorities shall be determined by each Party and submitted to the depositary at the time of depositing the notification of completion of domestic procedures required for the entry into force of this Agreement.

The Parties shall promptly notify the depositary of changes to the list of competent authorities.

3. If necessary, the competent authorities of the Parties may additionally determine the order of interaction and the list of persons authorized for its implementation, and directly notify each other thereof.

20. Cooperation on Training and Technical Assistance (including support for UNODC)

Article 29(2-4) UNTOC. Training and Technical Assistance

2. States Parties shall assist one another in planning and implementing research and training programmes designed to share expertise in the areas referred to in paragraph 1 of this article and to that end shall also, when appropriate, use regional and international conferences and seminars to promote cooperation and to stimulate discussion on problems of mutual concern, including the special problems and needs of transit States.

3. States Parties shall promote training and technical assistance that will facilitate extradition and mutual legal assistance. Such training and technical assistance may include language training, secondments and exchanges between personnel in central authorities or agencies with relevant responsibilities.

4. In the case of existing bilateral and multilateral agreements or arrangements, States Parties shall strengthen, to the extent necessary, efforts to maximize operational and training activities within international and regional organizations and within other relevant bilateral and multilateral agreements or arrangements.

Article 30 UNTOC. Other Measures: Implementation of the Convention through Economic Development and Technical Assistance

1. States Parties shall take measures conducive to the optimal implementation of this Convention to the extent possible, through international cooperation, taking into account the negative effects of organized crime on society in general, in particular on sustainable development.

2. States Parties shall make concrete efforts to the extent possible and in coordination with each other, as well as with international and regional organizations:

(*a*) To enhance their cooperation at various levels with developing countries, with a view to strengthening the capacity of the latter to prevent and combat transnational organized crime;

(*b*) To enhance financial and material assistance to support the efforts of developing countries to fight transnational organized crime effectively and to help them implement this Convention successfully;

(*c*) To provide technical assistance to developing countries and countries with economies in transition to assist them in meeting their needs for the implementation of this Convention. To that end, States Parties shall endeavour to make adequate and regular voluntary contributions to an account specifically designated for that purpose in a United Nations funding mechanism. States Parties may also give special consideration, in accordance with their domestic law and the provisions of this Convention, to contributing to the aforementioned account a percentage of the money or of the corresponding value of proceeds of crime or property confiscated in accordance with the provisions of this Convention;

(*d*) To encourage and persuade other States and financial institutions as appropriate to join them in efforts in accordance with this article, in particular by providing more training programmes and modern equipment to developing countries in order to assist them in achieving the objectives of this Convention.

3. To the extent possible, these measures shall be without prejudice to existing foreign assistance commitments or to other financial cooperation arrangements at the bilateral, regional or international level.

4. States Parties may conclude bilateral or multilateral agreements or arrangements on material and logistical assistance, taking into consideration the financial arrangements necessary for the means of international cooperation provided for by this Convention to be effective and for the prevention, detection and control of transnational organized crime.

Article 60(2)(3)(7)(8) UNCAC. Training and Technical Assistance

2. States Parties shall, according to their capacity, consider affording one another the widest measure of technical assistance, especially for the benefit of developing countries, in their respective plans and programmes to combat corruption, including material support and training in the areas referred to in paragraph 1 of this article, and training and assistance and the mutual exchange of relevant experience and specialized knowledge, which will facilitate international cooperation between States Parties in the areas of extradition and mutual legal assistance.

3. States Parties shall strengthen, to the extent necessary, efforts to maximize operational and training activities in international and regional organizations and in the framework of relevant bilateral and multilateral agreements or arrangements.

7. States Parties shall consider establishing voluntary mechanisms with a view to contributing financially to the efforts of developing countries and countries with economies in transition to apply this Convention through technical assistance programmes and projects.

8. Each State Party shall consider making voluntary contributions to the United Nations Office on Drugs and Crime for the purpose of fostering, through the Office, programmes and projects in developing countries with a view to implementing this Convention.

Article 62 UNCAC. Other Measures: Implementation of the Convention through Economic Development and Technical Assistance

1. States Parties shall take measures conducive to the optimal implementation of this Convention to the extent possible, through international cooperation, taking into account the negative effects of corruption on society in general, in particular on sustainable development.

2. States Parties shall make concrete efforts to the extent possible and in coordination with each other, as well as with international and regional organizations:

(*a*) To enhance their cooperation at various levels with developing countries, with a view to strengthening the capacity of the latter to prevent and combat corruption;

(*b*) To enhance financial and material assistance to support the efforts of developing countries to prevent and fight corruption effectively and to help them implement this Convention successfully;

(*c*) To provide technical assistance to developing countries and countries with economies in transition to assist them in meeting their needs for the implementation of this Convention. To that end, States Parties shall endeavour to make adequate and regular voluntary contributions to an account specifically designated for that purpose in a United Nations funding mechanism. States Parties may also give special consideration, in accordance with their domestic law and the provisions of this Convention, to contributing to that account a percentage of the money or of the corresponding value of proceeds of crime or property confiscated in accordance with the provisions of this Convention;

(*d*) To encourage and persuade other States and financial institutions as appropriate to join them in efforts in accordance with this article, in particular by providing more training programmes and modern equipment to developing countries in order to assist them in achieving the objectives of this Convention.

3. To the extent possible, these measures shall be without prejudice to existing foreign assistance commitments or to other financial cooperation arrangements at the bilateral, regional or international level.

4. States Parties may conclude bilateral or multilateral agreements or arrangements on material and logistical assistance, taking into consideration the financial arrangements necessary for the means of international cooperation provided for by this Convention to be effective and for the prevention, detection and control of corruption.

J. Preventive Measures, Cybersecurity Policies & Awareness-Raising

Paragraph 3 IEG Recommendations

UNODC should engage actively in capacity-building for all Member States in need of assistance, in particular developing countries. Such capacity-building activities should be politically neutral and free from conditions, should result from thorough consultations and be voluntarily accepted by the recipient countries. In terms of substance, those capacity-building activities should cover at least the following areas: training for judges, prosecutors, investigators and law enforcement authorities in cybercrime investigations, the handling of electronic evidence, chain of custody and forensic analysis.

Paragraph 7 IEG Recommendations

States are encouraged to continue to provide UNODC with the necessary mandates and financial support with a view to delivering tangible results in capacity-building projects in that area.

Paragraph 31 IEG Recommendations

UNODC is encouraged to further provide capacity-building and training programmes in combating cybercrime to national governmental experts to strengthen capacities to detect and investigate cybercrime. Such capacity-building should address the needs of developing countries, focus on the vulnerabilities of each country in order to provide tailor-made technical assistance and promote the exchange of the most up-to-date knowledge in the best interests of practitioners and stakeholders.

Paragraph 39 IEG Recommendations

It was recommended that the public should have easy access to prevention tools such as online platforms, audio clips, plain-language infographics and reporting platforms.

Paragraph 41 IEG Recommendations

When preventing and combating cybercrime, States should pay special attention to the issues of preventing and eradicating gender-based violence, in particular, violence against women and girls, and hate crimes.

Paragraph 44 IEG Recommendations

It was recommended that the collective capabilities of competent institutions be built and the prevention culture changed from reactive to proactive. It was also recommended that a robust mechanism to stimulate and facilitate the sharing of intelligence on potential criminal modi operandi be put in place.

Paragraph 46 IEG Recommendations

Owing to the existence of the "digital gap", some developing countries lack the capacity to prevent, detect and combat cybercrime and are more vulnerable in the face of cybercrime challenges

Paragraph 47 IEG Recommendations

UNODC was strongly encouraged to continue providing technical assistance, upon request, to prevent and counter cybercrime.

Paragraph 50 IEG Recommendations

Efforts in the development of strategies for cybercrime prevention should also take into account the protection of human rights.

Paragraph 51 IEG Recommendations

"Criminal justice capacity" should be another area of focus in national cybercrime strategies. Assistance to developing countries should be a priority in order to strengthen law enforcement capacity in preventing cybercrime.

Paragraph 59 IEG Recommendations

States should involve female experts in the prevention and investigation of cybercrime.

Paragraph 60 IEG Recommendations

National and regional prevention experiences should be brought together to create a multilateral repository that would allow the dissemination of good practices in diverse contexts.

Paragraph 63 IEG Recommendations

UNODC should facilitate the sharing of best practices on effective and successful preventive measures against cybercrime.

1. Prevention (including Awareness-Raising)

Paragraph 2 IEG Recommendations

Member States should support the United Nations Office on Drugs and Crime (UNODC) in establishing an educational project or programme that focuses on raising awareness of cybercrime and appropriate responses to it among judicial and prosecution authorities, digital forensic experts of Member States and among private entities, and use capacity-building tools or an electronic knowledge management platform to raise awareness of the impact of cybercrime among civil society.

Paragraph 14 IEG Recommendations

UNODC should establish an educational programme focused on raising knowledge and awareness of measures to counter cybercrime, especially in the sphere of electronic evidence gathering, for the judicial and prosecution authorities of Member States.

Paragraph 38 IEG Recommendations

It should be recognized that prevention is not just the responsibility of Governments: it also requires the participation of all relevant stakeholders, including law enforcement authorities, the private sector, especially Internet service providers, non-governmental organizations, schools and academia, in addition to the public in general.

Paragraph 40 IEG Recommendations

It was deemed necessary to develop a series of long-term public policies on prevention, which should include the development of awareness-raising campaigns on the safe use of the Internet.

Paragraph 48 IEG Recommendations

Member States are encouraged to continue to include effective prevention measures at the national and international levels and to focus on proactive activities, such as raising awareness about the risks of cybercrime and the likelihood of prosecution and punishment for offenders and efforts to prevent further crime, by identifying and disrupting ongoing illicit online activities.

Para. 61 IEG Recommendations

Greater awareness should be generated and legislative assistance should be provided on regulatory frameworks against cyberbullying and online threats of violence or abuse.

Article 31 UNTOC. Prevention

1. States Parties shall endeavour to develop and evaluate national projects and to establish and promote best practices and policies aimed at the prevention of transnational organized crime.

2. States Parties shall endeavour, in accordance with fundamental principles of their domestic law, to reduce existing or future opportunities for organized criminal groups to participate in lawful markets with proceeds of crime, through appropriate legislative, administrative or other measures. These measures should focus on:

(*a*) The strengthening of cooperation between law enforcement agencies or prosecutors and relevant private entities, including industry;

(*b*) The promotion of the development of standards and procedures designed to safeguard the integrity of public and relevant private entities, as well as codes of conduct for relevant professions, in particular lawyers, notaries public, tax consultants and accountants;

(*c*) The prevention of the misuse by organized criminal groups of tender procedures conducted by public authorities and of subsidies and licences granted by public authorities for commercial activity;

(*d*) The prevention of the misuse of legal persons by organized criminal groups; such measures could include:

(*i*) The establishment of public records on legal and natural persons involved in the establishment, management and funding of legal persons;

(*ii*) The introduction of the possibility of disqualifying by court order or any appropriate means for a reasonable period of time persons convicted of offences covered by this Convention from acting as directors of legal persons incorporated within their jurisdiction;

(*iii*) The establishment of national records of persons disqualified from acting as directors of legal persons; and

(*iv*) The exchange of information contained in the records referred to in subparagraphs (d) (i) and (iii) of this paragraph with the competent authorities of other States Parties.

3. States Parties shall endeavour to promote the reintegration into society of persons convicted of offences covered by this Convention.

4. States Parties shall endeavour to evaluate periodically existing relevant legal instruments and administrative practices with a view to detecting their vulnerability to misuse by organized criminal groups.

5. States Parties shall endeavour to promote public awareness regarding the existence, causes and gravity of and the threat posed by transnational organized crime. Information may be disseminated where appropriate through the mass media and shall include measures to promote public participation in preventing and combating such crime.

6. Each State Party shall inform the Secretary-General of the United Nations of the name and address of the authority or authorities that can assist other States Parties in developing measures to prevent transnational organized crime.

7. States Parties shall, as appropriate, collaborate with each other and relevant international and regional organizations in promoting and developing the measures referred to in this article. This includes participation in international projects aimed at the prevention of transnational organized crime, for example by alleviating the circumstances that render socially marginalized groups vulnerable to the action of transnational organized crime.

2. Analysis of Information

Paragraph 36 IEG Recommendations

Member States should consider maintaining electronic databases that facilitate access to statistics relating to incoming and outgoing requests for mutual legal assistance involving electronic evidence, to ensure that reviews of efficiency and effectiveness are in place.

Paragraph 53 IEG Recommendations

States should undertake surveys to measure the impact of cybercrime on businesses, including measures implemented, employee training, types of cyber-incidents that affect them and the costs associated with recovering from and preventing cyber-incidents.

Paragraph 56 IEG Recommendations

The modi operandi of contemporary cybercriminals should be carefully studied by means of intelligence analysis and criminological research in order to deploy existing resources more effectively and identify vulnerabilities.

Paragraph 49 IEG Recommendations

Countries should collect a broad range of data to help understand trends to inform and shape cybercrime policies and operational responses to combat cybercrime.

Article 28(1) UNTOC

1. Each State Party shall consider analysing, in consultation with the scientific and academic communities, trends in organized crime in its territory, the circumstances in which organized crime operates, as well as the professional groups and technologies involved.

Article 61(1) UNCAC. Collection, Exchange and Analysis of Information on Corruption

1. Each State Party shall consider analysing, in consultation with experts, trends in corruption in its territory, as well as the circumstances in which corruption offences are committed.

Article 60(4) UNCAC. Training and Technical Assistance

4. States Parties shall consider assisting one another, upon request, in conducting evaluations, studies and research relating to the types, causes, effects and costs of corruption in their respective countries, with a view to developing, with the participation of competent authorities and society, strategies and action plans to combat corruption.

3. Monitoring of Policies and Measures

Article 28(3) UNTOC. Collection, Exchange and Analysis of Information on the Nature of Organized Crime

3. Each State Party shall consider monitoring its policies and actual measures to combat organized crime and making assessments of their effectiveness and efficiency.

Article 61(3) UNCAC. Collection, Exchange and Analysis of Information on Corruption

3. Each State Party shall consider monitoring its policies and actual measures to combat corruption and making assessments of their effectiveness and efficiency.

Article 27(2) AU Convention 2014. National Cyber Security Monitoring Structures

2. Institutional framework

Each State Party shall adopt such measures as it deems necessary in order to establish appropriate institutions to combat cyber-crime, ensure monitoring and a response to incidents and alerts, national and cross-border coordination of cyber security problems, as well as global cooperation.

Article 32 AU Convention 2014. Measures to be Taken at the Level of the African Union

The Chairperson of the Commission shall report to the Assembly on the establishment and monitoring of the operational mechanism for this Convention.

The monitoring mechanism to be established shall ensure the following:

(*a*) Promote and encourage the Continent to adopt and implement measures to strengthen cyber security in electronic services and in combatting cybercrime and human rights violations in cyberspace;

(*b*) Gather documents and information on cyber security needs as well as on the nature and magnitude of cybercrime and human rights violations in cyberspace;

(*c*) Work out methods for analysing cyber security needs, as well as the nature and magnitude of cybercrime and human rights violations in cyberspace, disseminate information and sensitize the public on the negative effects of these phenomena;

(*d*) Advise African governments on the way to promote cyber security and combat the scourge of cybercrime and human rights violations in cyberspace at national level;

(*e*) Garner information and carry out analyses of the criminal behaviour of the users of information networks and computer systems operating in Africa, and transmit such information to competent national authorities;

(*f*) Formulate and promote the adoption of harmonized codes of conduct for the use of public officials in the area of cyber security;

(*g*) Establish partnerships with the Commission and the African Court on Human and Peoples' Rights, the African civil society, and governmental, intergovernmental and non-governmental organizations with a view to facilitating dialogue on combating cybercrime and human rights violations in cyberspace;

(*h*) Submit regular reports to the Executive Council of the African Union on the progress made by each State Party in the implementation of the provisions of this Convention;

(*i*) Carry out any other tasks relating to cybercrime and breaches of the rights of individuals in cyberspace as may be assigned to it by the policy organs of the African Union.

4. Development of a National Cybersecurity Framework

Article 24(1) AU Convention 2014. National Cyber Security Framework

1. National policy

Each State Party shall undertake to develop, in collaboration with stakeholders, a national cyber security policy which recognizes the importance of Critical Information Infrastructure (CII) for the nation identifies the risks facing the nation in using the all-hazards approach and outlines how the objectives of such policy are to be achieved.

Article 27 AU Convention 2014. National Cyber Security Monitoring Structures

1. Cyber security governance

(*a*) Each State Party shall adopt the necessary measures to establish an appropriate institutional mechanism responsible for cyber security governance;

(*b*) The measures adopted as per paragraph 1 of this Article shall establish strong leadership and commitment in the different aspects of cyber security institutions and relevant professional bodies of the State Party. To this end, State Parties shall take the necessary measures to:

(*i*) Establish clear accountability in matters of cyber security at all levels of Government by defining the roles and responsibilities in precise terms;

(*ii*) Express a clear, public and transparent commitment to cyber security;

(*iii*) Encourage the private sector and solicit its commitment and participation in government-led initiatives to promote cyber security.

(*c*) Cyber security governance should be established within a national framework that can respond to the perceived challenges and to all issues relating to information security at national level in as many areas of cyber security as possible.

2. Institutional framework

Each State Party shall adopt such measures as it deems necessary in order to establish appropriate institutions to combat cyber-crime, ensure monitoring and a response to incidents and alerts, national and cross-border coordination of cyber security problems, as well as global cooperation.

5. Protection of Critical Infrastructure

Article 25(4) AU Convention 2014. Legal Measures

4. Protection of critical infrastructure

Each State Party shall adopt such legislative and/or regulatory measures as they deem necessary to identify the sectors regarded as sensitive for their national security and well-being of the economy, as well as the information and communication technologies systems designed to function in these sectors as elements of critical information infrastructure; and, in this regard, proposing more severe sanctions for criminal activities on ICT systems in these sectors, as well as measures to improve vigilance, security and management.

6. Establish a Culture of Cybersecurity

Article 26(1) AU Convention 2014. National Cyber Security System

1. Culture of Cyber Security

(*a*) Each State Party undertakes to promote the culture of cyber security among all stakeholders, namely, governments, enterprises and the civil society, which develop, own, manage, operationalize and use information systems and networks. The culture of cyber security should lay emphasis on security in the development of information systems and networks, and on the adoption of new ways of thinking and behaving when using information systems as well as during communication or transactions across networks.

(*b*) As part of the promotion of the culture of cyber security, State Parties may adopt the following measures: establish a cyber security plan for the systems run by their governments; elaborate and implement programmes and initiatives for sensitization on security for systems and networks users; encourage the development of a cyber-security culture in enterprises; foster the involvement of the civil society; launch a comprehensive and detailed national sensitization programme for Internet users, small business, schools and children.

K. Protection of Informants and Victims

1. Protection of witnesses

Article 24 UNTOC. Protection of Witnesses

1. Each State Party shall take appropriate measures within its means to provide effective protection from potential retaliation or intimidation for witnesses in criminal proceedings who give testimony concerning offences covered by this Convention and, as appropriate, for their relatives and other persons close to them.

2. The measures envisaged in paragraph 1 of this article may include, inter alia, without prejudice to the rights of the defendant, including the right to due process:

(*a*) Establishing procedures for the physical protection of such persons, such as, to the extent necessary and feasible, relocating them and permitting, where appropriate, non-disclosure or limitations on the disclosure of information concerning the identity and whereabouts of such persons;

(*b*) Providing evidentiary rules to permit witness testimony to be given in a manner that ensures the safety of the witness, such as permitting testimony to be given through the use of communications technology such as video links or other adequate means.

3. States Parties shall consider entering into agreements or arrangements with other States for the relocation of persons referred to in paragraph 1 of this article.

4. The provisions of this article shall also apply to victims insofar as they are witnesses.

Article 32 UNCAC. Protection of Witnesses, Experts and Victims

1. Each State Party shall take appropriate measures in accordance with its domestic legal system and within its means to provide effective protection from potential retaliation or intimidation for witnesses and experts who give testimony concerning offences established in accordance with this Convention and, as appropriate, for their relatives and other persons close to them.

2. The measures envisaged in paragraph 1 of this article may include, inter alia, without prejudice to the rights of the defendant, including the right to due process:

(*a*) Establishing procedures for the physical protection of such persons, such as, to the extent necessary and feasible, relocating them and permitting, where

appropriate, non-disclosure or limitations on the disclosure of information concerning the identity and whereabouts of such persons;

(*b*) Providing evidentiary rules to permit witnesses and experts to give testimony in a manner that ensures the safety of such persons, such as permitting testimony to be given through the use of communications technology such as video or other adequate means.

3. States Parties shall consider entering into agreements or arrangements with other States for the relocation of persons referred to in paragraph 1 of this article.

4. The provisions of this article shall also apply to victims insofar as they are witnesses.

5. Each State Party shall, subject to its domestic law, enable the views and concerns of victims to be presented and considered at appropriate stages of criminal proceedings against offenders in a manner not prejudicial to the rights of the defence.

2. Protection of reporting persons

Article 33 UNCAC. Protection of Reporting Persons

Each State Party shall consider incorporating into its domestic legal system appropriate measures to provide protection against any unjustified treatment for any person who reports in good faith and on reasonable grounds to the competent authorities any facts concerning offences established in accordance with this Convention.

3. Assistance to and protection of victims

Paragraph 52 IEG Recommendations

States should develop or strengthen support programmes for victims of cybercrime.

Article 25 UNTOC. Assistance to and Protection of Victims

1. Each State Party shall take appropriate measures within its means to provide assistance and protection to victims of offences covered by this Convention, in particular in cases of threat of retaliation or intimidation.

2. Each State Party shall establish appropriate procedures to provide access to compensation and restitution for victims of offences covered by this Convention.

3. Each State Party shall, subject to its domestic law, enable views and concerns of victims to be presented and considered at appropriate stages of criminal proceedings against offenders in a manner not prejudicial to the rights of the defence.

L. Final Provisions

1. Implementation of the Convention

Article 34 UNTOC. Implementation of the Convention

1. Each State Party shall take the necessary measures, including legislative and administrative measures, in accordance with fundamental principles of its domestic law, to ensure the implementation of its obligations under this Convention.

2. The offences established in accordance with articles 5, 6, 8 and 23 of this Convention shall be established in the domestic law of each State Party independently of the transnational nature or the involvement of an organized criminal group as described in article 3, paragraph 1, of this Convention, except to the extent that article 5 of this Convention would require the involvement of an organized criminal group.

3. Each State Party may adopt more strict or severe measures than those provided for by this Convention for preventing and combating transnational organized crime.

Article 65 UNCAC. Implementation of the Convention

1. Each State Party shall take the necessary measures, including legislative and administrative measures, in accordance with fundamental principles of its domestic law, to ensure the implementation of its obligations under this Convention.

2. Each State Party may adopt more strict or severe measures than those provided for by this Convention for preventing and combating corruption.

2. Settlement of Disputes

Article 35 UNTOC. Settlement of Disputes

l. States Parties shall endeavour to settle disputes concerning the interpretation or application of this Convention through negotiation.

2. Any dispute between two or more States Parties concerning the interpretation or application of this Convention that cannot be settled through negotiation within a reasonable time shall, at the request of one of those States Parties, be submitted to arbitration. If, six months after the date of the request for arbitration, those States Parties are unable to agree on the organization of the arbitration, any one of those States Parties may refer the dispute to the International Court of Justice by request in accordance with the Statute of the Court.

3. Each State Party may, at the time of signature, ratification, acceptance or approval of or accession to this Convention, declare that it does not consider itself bound by paragraph 2 of this article. The other States Parties shall not be bound by paragraph 2 of this article with respect to any State Party that has made such a reservation.

4. Any State Party that has made a reservation in accordance with paragraph 3 of this article may at any time withdraw that reservation by notification to the Secretary-General of the United Nations.

Article 66 UNCAC. Settlement of Disputes

l. States Parties shall endeavour to settle disputes concerning the interpretation or application of this Convention through negotiation.

2. Any dispute between two or more States Parties concerning the interpretation or application of this Convention that cannot be settled through negotiation within a reasonable time shall, at the request of one of those States Parties, be submitted to arbitration. If, six months after the date of the request for arbitration, those States Parties are unable to agree on the organization of the arbitration, any one of those States Parties may refer the dispute to the International Court of Justice by request in accordance with the Statute of the Court.

3. Each State Party may, at the time of signature, ratification, acceptance or approval of or accession to this Convention, declare that it does not consider itself bound by paragraph 2 of this article. The other States Parties shall not be bound by paragraph 2 of this article with respect to any State Party that has made such a reservation.

4. Any State Party that has made a reservation in accordance with paragraph 3 of this article may at any time withdraw that reservation by notification to the Secretary-General of the United Nations.

Article 45 Budapest Convention. Settlement of Disputes

1. The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2. In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the

CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 34 AU Convention 2014. Settlement of Disputes

1. Any dispute arising from this Convention shall be settled amicably through direct negotiations between the State Parties concerned.

2. Where the dispute cannot be resolved through direct negotiation, the State Parties shall endeavour to resolve the dispute through other peaceful means, including good offices, mediation and conciliation, or any other peaceful means agreed upon by the State Parties. In this regard, the State Parties shall be encouraged to make use of the procedures and mechanisms for resolution of disputes established within the framework of the Union.

Article 9 Shanghai Cooperation Organization Agreement. Dispute Resolution

Disputes over interpretation and application of this Agreement shall be resolved through consultation and negotiations of the Parties.

Article 14 Dushanbe Agreement. Dispute Resolution

Disagreements arising during the application and interpretation of this Agreement shall be resolved through consultations and negotiations between the Parties concerned.

3. Signature, Ratification, Acceptance, Approval and Accession

Article 36 UNTOC. Signature, Ratification, Acceptance, Approval and Accession

1. This Convention shall be open to all States for signature from 12 to 15 December 2000 in Palermo, Italy, and thereafter at United Nations Headquarters in New York until 12 December 2002.

2. This Convention shall also be open for signature by regional economic integration organizations provided that at least one member State of such organization has signed this Convention in accordance with paragraph 1 of this article.

3. This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary-General of the United Nations. A regional economic integration organization may deposit its instrument of ratification, acceptance or approval if at least one of its member States has done likewise. In that instrument of ratification, acceptance or approval, such organization shall declare the extent of its competence with respect to the matters governed by this Convention. Such organization shall also inform the depositary of any relevant modification in the extent of its competence.

4. This Convention is open for accession by any State or any regional economic integration organization of which at least one member State is a Party to this Convention. Instruments of accession shall be deposited with the Secretary-General of the United Nations. At the time of its accession, a regional economic integration organization shall declare the extent of its competence with respect to matters governed by this Convention. Such organization shall also inform the depositary of any relevant modification in the extent of its competence.

*Article 67 UNCAC. Signature, Ratification, Accept*ance, Approval and Accession

1. This Convention shall be open to all States for signature from 9 to 11 December 2003 in Merida, Mexico, and thereafter at United Nations Headquarters in New York until 9 December 2005.

2. This Convention shall also be open for signature by regional economic integration organizations provided that at least one member State of such organization has signed this Convention in accordance with paragraph 1 of this article.

3. This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary-General of the United Nations. A regional economic integration organization may deposit its instrument of ratification, acceptance or approval if at least one of its member States has done likewise. In that instrument of ratification, acceptance or approval, such organization shall declare the extent of its competence with respect to the matters governed by this Convention. Such organization shall also inform the depositary of any relevant modification in the extent of its competence.

4. This Convention is open for accession by any State or any regional economic integration organization of which at least one member State is a Party to this Convention. Instruments of accession shall be deposited with the Secretary-General of the United Nations. At the time of its accession, a regional economic integration organization shall declare the extent of its competence with respect to matters governed by this Convention. Such organization shall also inform the depositary of any relevant modification in the extent of its competence.

Article 36 Budapest Convention. Signature and Entry into Force

1. This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2. This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3. This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4. In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 Budapest Convention. Accession to the Convention

1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2. In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 35 AU Convention 2014. Signature, Ratification or Accession

This Convention shall be open to all Member States of the Union, for signature, ratification or accession, in conformity with their respective constitutional procedures.

Article 12(3) SCO Agreement. Final Provisions

3. This Agreement is not directed against any state and organization and after its entry into force it shall be open for accession by any state that shares the goals and

principles of this Agreement by submission to the Depositary of an instrument of accession. For the acceding state, the present Agreement shall enter into force in thirty days after the date of the receipt by the Depositary of the last notification of acceptance of the accession by the signatory and acceded states.

Article 16 Dushanbe Agreement. Accession

This Agreement, once it enters into force, is open for accession by any State Party to the Commonwealth of Independent States by means of the deposit of an instrument of accession. For the acceding State, the Agreement shall enter into force 30 days after the date of receipt by the depositary of the instrument of accession.

4. Relation with Protocols

Article 37 UNTOC. Relation with Protocols

1. This Convention may be supplemented by one or more protocols.

2. In order to become a Party to a protocol, a State or a regional economic integration organization must also be a Party to this Convention.

3. A State Party to this Convention is not bound by a protocol unless it becomes a Party to the protocol in accordance with the provisions thereof.

4. Any protocol to this Convention shall be interpreted together with this Convention, taking into account the purpose of that protocol.

5. Entry into Force

Article 38 UNTOC. Entry into Force

1. This Convention shall enter into force on the ninetieth day after the date of deposit of the fortieth instrument of ratification, acceptance, approval or accession. For the purpose of this paragraph, any instrument deposited by a regional economic integration organization shall not be counted as additional to those deposited by member States of such organization.

2. For each State or regional economic integration organization ratifying, accepting, approving or acceding to this Convention after the deposit of the fortieth instrument of such action, this Convention shall enter into force on the thirtieth day after the date of deposit by such State or organization of the relevant instrument.

Article 68 UNCAC. Entry into Force

1. This Convention shall enter into force on the ninetieth day after the date of deposit of the thirtieth instrument of ratification, acceptance, approval or accession. For the purpose of this paragraph, any instrument deposited by a regional economic integration organization shall not be counted as additional to those deposited by member States of such organization.

2. For each State or regional economic integration organization ratifying, accepting, approving or acceding to this Convention after the deposit of the thirtieth instrument of such action, this Convention shall enter into force on the thirtieth day after the date of deposit by such State or organization of the relevant instrument or on the date this Convention enters into force pursuant to paragraph 1 of this article, whichever is later.

Article 36 Budapest Convention. Signature and Entry into Force

1. This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2. This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3. This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4. In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 36 AU Convention 2014. Entry into Force

This Convention shall enter into force thirty (30) days after the date of the receipt by the Chairperson of the Commission of the African Union of the fifteenth (15^{th}) instrument of ratification.

Article 12(1) SCO Agreement. Final Provisions

1. This Agreement is concluded for an indefinite period and it shall enter into force on the thirtieth day after the date of receipt by the Depositary of the fourth written notification of the completion of their internal procedures necessary for its entry into force. In respect of the Party that have completed internal procedures later, this Agreement shall enter into force on the thirtieth day after the date of the receipt by the Depositary of a respective notice.

Article 17 Dushanbe Agreement. Entry into Force

1. This Agreement shall enter into force 30 days after the date of receipt by the depositary of the third notification on completion by the signatories of domestic procedures necessary for its entry into force.

For the Parties which have executed domestic procedures later, this Agreement comes into force after 30 days from the date of receipt of appropriate documents by the depositary.

2. In relations between the States Parties to this Agreement, the Agreement on cooperation of the States Parties of the Commonwealth of Independent States in combating crimes in the field of computer information of 1 June 2001 shall cease to be in force from the date of entry into force of this Agreement.

6. Territorial Application

Article 38 Budapest Convention. Territorial Application

1. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2. Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

7. Declarations

Article 40 Budapest Convention. Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

8. Federal Clause

Article 41 Budapest Convention. Federal Clause

1. A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2. When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3. With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

9. Reservations

Article 42 Budapest Convention. Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

10. Status and Withdrawal of Reservations

Article 43 Budapest Convention. Status and Withdrawal of Reservations

1. A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2. A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3. The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

11. Amendment

Article 39 UNTOC. Amendment

1. After the expiry of five years from the entry into force of this Convention, a State Party may propose an amendment and file it with the Secretary-General of the United Nations, who shall thereupon communicate the proposed amendment to the States Parties and to the Conference of the Parties to the Convention for the purpose of considering and deciding on the proposal. The Conference of the Parties shall make every effort to achieve consensus on each amendment. If all efforts at consensus have been exhausted and no agreement has been reached, the amendment shall, as a last resort, require for its adoption a two-thirds majority vote of the States Parties present and voting at the meeting of the Conference of the Parties.

2. Regional economic integration organizations, in matters within their competence, shall exercise their right to vote under this article with a number of votes equal to the number of their member States that are Parties to this Convention. Such organizations shall not exercise their right to vote if their member States exercise theirs and vice versa.

3. An amendment adopted in accordance with paragraph 1 of this article is subject to ratification, acceptance or approval by States Parties.

4. An amendment adopted in accordance with paragraph 1 of this article shall enter into force in respect of a State Party ninety days after the date of the deposit with the Secretary-General of the United Nations of an instrument of ratification, acceptance or approval of such amendment.

5. When an amendment enters into force, it shall be binding on those States Parties which have expressed their consent to be bound by it. Other States Parties shall still be bound by the provisions of this Convention and any earlier amendments that they have ratified, accepted or approved.

Article 69 UNCAC. Amendment

1. After the expiry of five years from the entry into force of this Convention, a State Party may propose an amendment and transmit it to the Secretary-General of the United Nations, who shall thereupon communicate the proposed amendment to the States Parties and to the Conference of the States Parties to the Convention for the purpose of considering and deciding on the proposal. The Conference of the States Parties shall make every effort to achieve consensus on each amendment. If all efforts at consensus have been exhausted and no agreement has been reached, the amendment shall, as a last resort, require for its adoption a two-thirds majority vote of the States Parties present and voting at the meeting of the Conference of the States Parties.

2. Regional economic integration organizations, in matters within their competence, shall exercise their right to vote under this article with a number of votes equal to the number of their member States that are Parties to this Convention. Such organizations shall not exercise their right to vote if their member States exercise theirs and vice versa.

3. An amendment adopted in accordance with paragraph 1 of this article is subject to ratification, acceptance or approval by States Parties.

4. An amendment adopted in accordance with paragraph 1 of this article shall enter into force in respect of a State Party ninety days after the date of the deposit with the Secretary-General of the United Nations of an instrument of ratification, acceptance or approval of such amendment.

5. When an amendment enters into force, it shall be binding on those States Parties which have expressed their consent to be bound by it. Other States Parties shall still be bound by the provisions of this Convention and any earlier amendments that they have ratified, accepted or approved.

Article 44 Budapest Convention. Amendments

1. Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2. Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3. The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

4. The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5. Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 37 AU Convention 2014. Amendment

1. Any State Party may submit proposals for the amendment or revision of this Convention;

2. Proposals for amendment or revision shall be submitted to the Chairperson of the Commission of the African Union, who shall transmit same to State Parties within thirty (30) days of receipt thereof;

3. The Assembly of the Union, upon recommendation of the Executive Council of the Union, shall consider these proposals at its next session, provided all State Parties have been notified at least three (3) months before the beginning of the session;

4. The Assembly of the Union shall adopt the amendments in accordance with its Rules of Procedure;

5. The amendments or revisions shall enter into force in accordance with the provisions of Article 36 above.

*Article 12(2) SCO Agr*eement. Final Provisions

2. The Parties may amend this Agreement by issuing separate protocols by mutual consent of the Parties.

Article 15 Dushanbe Agreement. Amendments and Additions

By agreement of the Parties, this Agreement may be amended and supplemented as an integral part thereof, which shall be executed by the appropriate protocol.

12. Denunciation

Article 40 UNTOC. Denunciation

1. A State Party may denounce this Convention by written notification to the Secretary-General of the United Nations. Such denunciation shall become effective one year after the date of receipt of the notification by the Secretary-General.

2. A regional economic integration organization shall cease to be a Party to this Convention when all of its member States have denounced it.

3. Denunciation of this Convention in accordance with paragraph 1 of this article shall entail the denunciation of any protocols thereto.

Article 70 UNCAC. Denunciation

1. A State Party may denounce this Convention by written notification to the Secretary-General of the United Nations. Such denunciation shall become effective one year after the date of receipt of the notification by the Secretary-General.

2. A regional economic integration organization shall cease to be a Party to this Convention when all of its member States have denounced it.

Article 47 Budapest Convention. Denunciation

1. Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2. Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 12(4)(5) SCO Agreement. Final Provisions

4. Each Party may withdraw from this Agreement by sending to the Depositary a written notice at least ninety days prior to the intended date of withdrawal. The Depositary shall notify the other Parties of such intention within thirty days from the date of receipt of such notice.

5. In the event of termination of this Agreement, the Parties shall take measures to fully meet the commitments in respect of the protection of information, as well as complete previously agreed joint work, projects and other activities carried out in the framework of the Agreement and uncompleted by the time of the Agreement termination.

13. Notification

Article 48 Budapest Convention. Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

(*a*) any signature;

(*b*) the deposit of any instrument of ratification, acceptance, approval or accession;

(*c*) any date of entry into force of this Convention in accordance with Articles 36 and 37;

(*d*) any declaration made under Article 40 or reservation made in accordance with Article 42;

(*e*) any other act, notification or communication relating to this Convention.

14. Depositary and Languages

Article 41 UNTOC. Depositary and Languages

1. The Secretary-General of the United Nations is designated depositary of this Convention.

2. The original of this Convention, of which the Arabic, Chinese, English, French, Russian and Spanish texts are equally authentic, shall be deposited with the Secretary-General of the United Nations.

Article 71 UNCAC. Depositary and Languages

1. The Secretary-General of the United Nations is designated depositary of this Convention.

2. The original of this Convention, of which the Arabic, Chinese, English, French, Russian and Spanish texts are equally authentic, shall be deposited with the Secretary-General of the United Nations.

Budapest Convention

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.

Article 38 AU Convention 2014. Depository

1. The instruments of ratification or accession shall be deposited with the Chairperson of the Commission of the African Union;

2. Any State Party may withdraw from this Convention by giving a written notice one (1) year in advance to the Chairperson of the Commission of the African Union;

3. The Chairperson of the Commission of the African Union shall inform all Member States of any signature, depositing of instrument of ratification or accession to this Convention, as well as its entry into force;

4. The Chairperson of the Commission shall also inform the State Parties of requests for amendments or withdrawal from the Convention, as well as reservations thereon.

5. Upon entry into force of this Convention, the Chairperson of the Commission shall register it with the Secretary General of the United Nations, in accordance with Article 102 of the Charter of the United Nations.

6. This Convention, drawn up in four (4) original texts in Arabic, English, French and Portuguese languages, all four (4) texts being equally authentic, shall be deposited with the Chairperson of the Commission who shall transmit certified true copies of the same to all Member States of the African Union in its official language.

*Article 11 SCO Agree*ment. Depositary

The Secretariat of the Shanghai Cooperation Organization shall be the Depositary of this Agreement.

The original of this Agreement shall be deposited with the Depositary that within fifteen days from the date of its signing will send the certified copies thereof to the Parties.