South Africa's contribution on the provisions on criminalisation, the general provisions and the provisions on procedural measures and law enforcement

Preamble

The Government of the Republic of South Africa welcomes the invitation to contribute to the provisions on **criminalisation**, **the general provisions** and the provisions on **procedural measures and law enforcement.** South Africa reiterates the complementarity of the future Convention and existing instruments such as UNTOC and UNCAC. We further welcome the chapter-by-chapter negotiation process which allow delegations to provide meaningful contributions towards the elaboration of a comprehensive International Convention on countering the use of information and communications technologies for criminal purposes. In this regard, South Africa submits contributions on the first three Chapters as per the adopted Structure of the future Convention as follows:

Chapter I
General provisions

Article 1 Statement on objectives

The objectives of the Convention shall be:

(a) To promote and strengthen measures to prevent and combat the use of information and

communications technologies for criminal purposes/cybercrime, while protecting information and communications technologies users from such crime.

(b) To promote and strengthen measures aimed at effectively preventing and combating crimes and other unlawful acts in the field of information and communications technologies.

(c) To promote, facilitate and support international cooperation in preventing and combating the use of information and communications technologies for criminal purposes/cybercrime.

(d) To provide practical tools to enhance technical assistance among States Parties and build the capacity of national authorities to prevent and combat the use of information and communications technologies for criminal purposes/cybercrime, and strengthen measures to promote the exchange of information, experiences and good practices.

Article 2 Use of terms

For the purposes of this Convention:

‘‘article’’ means any—

(a) data;

(b) computer program;

(c) computer data storage medium; or

(d) computer system,

which—

(i) is concerned with, connected with or is, on reasonable grounds, believed to be concerned with or connected with the commission or suspected commission;

(ii) may afford evidence of the commission or suspected commission; or

(iii) is intended to be used or is, on reasonable grounds believed to be intended to be used in the commission or intended commission, of—

(aa) an offence in terms of this Convention;

(bb) any other offence brought about through the use of information and communications technologies; or

(cc) an offence in a foreign State that is substantially similar to an offence contemplated in this Convention;

“child sexual abuse materials" means any image, however created, or any description or presentation, 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; and

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

‘‘computer’’ means any electronic programmable device used, whether by itself or as part of a computer system or any other device or equipment, or any part thereof, to perform predetermined arithmetic, logical, routing, processing or storage operations in accordance with set instructions and includes any data, computer program or computer data storage medium that are related to, connected with or used with such a device;

"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;

‘‘computer data storage medium’’ means any device from which data or a computer program is capable of being reproduced or on which data or a computer program is capable of being stored, by a computer system, irrespective of whether the device is physically attached to or connected with a computer system;

‘‘computer program’’ means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;

‘‘computer system’’ means—

(a) one computer; or

(b) two or more inter-connected or related computers, which allow these inter-connected or related computers to—

(i) exchange data or any other function with each other; or

(ii) exchange data or any other function with another computer or a computer system;

“confiscation”, which includes forfeiture where applicable, shall mean the permanent deprivation of property by order of a court or other competent authority;

"

"cyber dependant crimes" are offences that can only be committed using a computer, computer networks or other form of information communications technology;

"cyber enabled crimes" are crimes which do not depend on computers or networks but have been transformed in scale or form by the use of the internet and communications technology.

‘‘data message’’ means data generated, sent, received or stored by electronic means, where any output of the data is in an intelligible form;

"digital information" means any data (records), irrespective of form and characteristics, contained and processed in information and communication devices, systems and networks;

"electronic evidence" shall mean any evidentiary information stored or transmitted in digital form (on an electronic medium);

“freezing of assets” 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;

“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;

“proceeds of crime” shall mean any property derived from or obtained, directly or indirectly, through the commission of an offence;

“predicate offence” shall mean any offence as a result of which proceeds have been generated that may become the subject of an offence as defined in article 23 of this Convention and domestic legislation of State Party/Member State;

"seizure of assets" shall mean taking permanent control of the assets or permanent assumption of custody or control of property on the basis of an order issued by a court or other competent authority;

“service provider” means any public or private entity that provides to users of its service the ability to communicate by means of a computer system, or any other entity that processes or stores computer data on behalf of such communication service or users of such service.

“traffic data” means data relating to a communication indicating the communication’s origin, destination, route, format, time, date, size, duration or type, of the underlying service.

Article 3 Scope of application

This Convention shall apply**,** in accordance with its terms, to the prevention, investigation and prosecution of cyber dependent and/or specific cyber enabled crimes brought about by the use of information and communications technologies for criminal purposes and to the freezing, seizure, confiscation and return of the proceeds of offences established in accordance with this Convention.

Article 4 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.

Chapter II
Criminalization

Article 5 Illegal access

Each State 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 unlawfully, the illegal 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 unlawfully obtaining computer data or other

dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 6 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 and unlawfully, 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 Unauthorized interference with digital information

1. Each State 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 unlawfully, 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 (to natural persons, juristic persons and the economy of a State Party).

Article 8 System interference and disruption of information and communication networks

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 unlawfully, the serious hindering without right of the functioning of a computer

system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 9 Creation, utilization and distribution of devices

1. Each State 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 unlawfully 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 5 through 26;

(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 5 through 26; 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 5 through 26. 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

5 through 26 of this Convention, such as for the authorised testing or protection of a computer system.

3. Each State 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 10 Cyber enabled forgery

Each State 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 unlawfully 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 11 Cyber enabled fraud

Each State 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 unlawfully 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 12 – Offences related to child sexual abuse materials

1. Each State 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 unlawfully, the following conduct:

(a) producing child sexual abuse materials for the purpose of its distribution through a computer system or information and communications technologies;

(b) offering or making available child sexual abuse materials through a computer system or information and communications technologies;

(c) distributing or transmitting child sexual abuse materials through a computer system or information and communications technologies;

(d) procuring child sexual abuse materials through a computer system or information and communications technologies for oneself or for another person;

(e) possessing child sexual abuse materials in a computer system or information and communications technologies or on a computer-data storage medium.

2 For the purpose of paragraph 1 above, the term "child sexual abuse materials" shall include material that visually depicts:

(a) minor engaged in sexually explicit conduct;

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

(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.

Article 13 – Offences related to infringements of copyright and related rights

1. Each State 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 various international treaties and agreements, 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 or information and communications technologies .

2. Each State 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 or information and communications technologies.

3. A State 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 14 Offences related to the distribution of narcotic drugs and psychotropic substances

Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal

offense under its domestic law acts, involving the use of information and communications technologies, that further the trafficking in narcotic drugs, psychotropic substances and materials required for their manufacture.

Article 15 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 involving the use of information and communications technologies established in accordance with this Convention.

Each State Party shall consider incorporating into its domestic legislation indemnity from prosecution, subject to satisfying standards/conditions adopted by a Party, of anyone providing full cooperation and in good faith when interacting with relevant law enforcement agencies.

Article 16 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 involving the use of information and communications technologies established in accordance with this Convention to supply information in good faith which is 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, in good faith, substantial cooperation in the investigation and prosecution of an offence involving the use of information and communications technologies 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, in good faith, provides substantial cooperation in the investigation or prosecution of an offence involving the use of information and communications technologies established in accordance with this Convention.

4. Protection of such persons shall be, *mutatis mutandis*, as provided for in article 22 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.

6. Each State Party shall maintain a register with identifiable information of all Domain name registrars, Crypto Asset Traders and Crypto Assets within its jurisdiction, in accordance with fundamental principles of its domestic law, and supply such information to competent authorities for investigative and evidentiary purpose

Article 17 Jurisdiction

1. Each State Party shall adopt such measures as may be necessary to establish its jurisdiction over the offences involving the use of information and communications

technologies 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.

2. Subject to article 4 of this Convention, a State Party may also establish its jurisdiction over any such offence involving the use of information and communications technologies when:

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

(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; or

(c) The offence is one of those established in accordance with article 17, paragraph 1 *(b)* (ii), of this Convention and is committed outside its territory with a view to the commission of an offence involving the use of information and communications technologies established in accordance with article 15 of this Convention within its territory; or

(d) The offence is committed against the State Party, or has direct impact on the affairs of such State Party.

3. For the purposes of article -–[on Extradition] of this Convention, each State Party shall take such measures as may be necessary to establish its jurisdiction over the offences involving the use of information and communications technologies 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 involving the use of information and communications technologies established in accordance with this Convention when the alleged offender is present in its territory and it does not extradite him or her.

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.

6. Without prejudice to norms of general international law, this Convention shall not exclude the exercise of any criminal jurisdiction established by a State Party in accordance with its domestic law.

Chapter III
Procedural measures and law enforcement

Article 18 – Procedural provisions

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

2. Except as specifically provided otherwise in Article 32, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

(a) the criminal offences involving the use of information and communications technologies established in accordance with Articles --- through --- of this Convention;

(b) other criminal offences committed by means of information and communications technologies; and

(c) the collection of evidence in electronic form of a criminal offence involving the use of information and communications technologies.

3. Each State Party may reserve the right to apply the measures referred to in Article 31 only to offences or categories of offences involving the use of information and communications technologies 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 32. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Article 31.

4. Where a State Party, due to limitations in its legislation in force at the time of the adoption of this Convention, is not able to apply the measures referred to in Articles 31 and 32 to communications being transmitted using information and communications technologies of a service provider, which system:

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

(b) does not employ public communications networks and is not connected with other information and communications technologies,

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 31 and 32.

Article 19 – Conditions and safeguards

1. Each State Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this article 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 and fundamental freedoms arising pursuant to obligations it has undertaken under agreements, treaties, applicable international human rights instruments, and which shall incorporate the principle of proportionality consistent with the sovereignty of the State Party.

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 article upon the rights, responsibilities and legitimate interests of third parties.

Article 20 Expedited preservation of stored computer data

1. Each State 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 information and communications technologies, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2. Where a State 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 7 days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3. Each State 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 27 and 28.

Article 21 Search and seizure of stored computer data

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

(a) information and communications technologies, 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 State Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access any information and communications technologies or components which form part of such technologies, 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 information and communications technologies or components forming part of such technologies, 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.

3. Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities, where applicable with the assistance or in the presence of the authorised officers of the foreign/other State Party 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 information and communications technologies or components forming part of such technologies, 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 or information and communications technologies.

4. Each State 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 information and communications technologies or components forming part of such technologies, a 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.

5. The powers and procedures referred to in this article shall be subject to Articles 27 and 28.

Article 22 Real-time collection of traffic data

1. Each State 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

information and communications technologies or a computer system.

Article 23 Interception of content data

1. Each State 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 information and communications technologies 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 27 and 28.

Article 24 Freezing, seizure and confiscation

1. Notwithstanding the fact that the provisions of this article it shall not be so construed as to prejudice the rights of bona fide third parties and that nothing contained in this article shall affect the principle that the measures to which it refers shall be defined and implemented in accordance with and subject to the provisions of the domestic law of a State Party.

2. The provisions of this article shall not be so construed as to prejudice the rights of *bona fide* third parties.

3. Nothing contained in this article shall affect the principle that the measures to which it refers shall be defined and implemented in accordance with and subject to the provisions of the domestic law of a State Party.

4. Each State Party shall take, to the greatest extent possible within its domestic legal system, such measures as may be necessary to enable confiscation of:

(a) Proceeds of crime derived from offences caused by the use of information and communication technologies established in accordance with this Convention or property the value of which corresponds to that of such proceeds and to the benefit of the affected State Party;

(b) Property, equipment or other instrumentalities including the use of information and communications technologies used in or

destined for use in offences established in accordance with this Convention.

4. Each State Party shall take such measures as may be necessary to enable the identification, tracing, freezing or seizure of any item referred to in paragraph 1 of this article for the purpose of eventual confiscation.

5. Each State Party shall adopt, in accordance with its domestic law, such legislative and other measures as may be necessary to regulate the administration by the competent authorities of frozen, seized or confiscated property covered in paragraphs 1 and 2 of this article.

6. If such proceeds of crime have been transformed or converted, in part or in full, into other property, such property shall be liable to the measures referred to in this article instead of the proceeds.

7. If such proceeds of crime have been intermingled with property acquired from legitimate sources, such property shall, without prejudice to any powers relating to freezing or seizure, be liable to confiscation up to the assessed value of the intermingled proceeds.

8. Income or other benefits derived from such proceeds of crime, from property into which such proceeds of crime have been transformed or converted or from property with which such proceeds of crime have been intermingled shall also be liable to the measures referred to in this article, in the same manner and to the same extent as proceeds of crime.

9. For the purpose of this article and article----[on international cooperation] of this Convention, each State Party shall empower its courts or other competent authorities to order that bank, financial or commercial records be made available or

seized. A State Party shall not decline to act under the provisions of this paragraph on the ground of bank secrecy.

10. States Parties may consider the possibility of requiring that an offender demonstrate the lawful origin of such alleged proceeds of crime or other property liable to confiscation, to the extent that such a requirement is consistent with the fundamental principles of their domestic law and with the nature of judicial and other proceedings.

Article 25 Disposal of confiscated proceeds of crime or property

1. Proceeds of crime or property confiscated by a State Party pursuant to article 33, paragraph 3, of this Convention shall be disposed of by that State Party in accordance with its domestic law and administrative procedures.

2. When acting on the request made by another State Party in accordance with article 39 of this Convention, States Parties shall, to the extent permitted by domestic law and if so requested, give priority consideration to returning the confiscated proceeds of crime or property to the requesting State Party so that it can give compensation to the victims of the crime or return such proceeds of crime or property to their legitimate owners.

3. When acting on the request made by another State Party in accordance with article 41 of this Convention, a State Party may give special consideration to concluding agreements or arrangements on:

(a) Contributing the value of such proceeds of crime or property or funds derived from the sale of

such proceeds of crime or property or a part thereof to the account designated in accordance with [article ----], of this Convention and to intergovernmental bodies specializing in the fight against organized crime;

(b) Sharing with other States Parties, on a regular or case-by-case basis, such proceeds of crime or property, or funds derived from the sale of such proceeds of crime or property, in accordance with its domestic law or administrative procedures.

Article 26 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 caused by the use of information and communications technologies established in accordance with this Convention.

Article 27 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, in good faith, 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, in good faith, substantial cooperation in the investigation or prosecution of an offence involving the use of information and communications technologies covered by this Convention.

4. Protection of such persons shall be as provided for in article 34 of this Convention.

5. Where a person referred to in paragraph 1 of this article located in one State Party can, in good faith, 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 28 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 involving the use of information and communications technologies 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 internet service providers in order to facilitate the secure and rapid exchange of information concerning all aspects of the offences involving the use of information and communications technologies 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 enquiries with respect to offences involving the use of information and communications technologies 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 internet service providers and to promote the exchange of personnel and other experts, including, subject to bilateral agreements or arrangements between the States Parties concerned;

(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 through the use of information and communications technologies;

(f) To exchange information and coordinate administrative and other measures taken as appropriate for the purpose of early identification of the offences involving the use of information and communications technologies 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 information and communications technologies.

Article 29 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 30 Special investigative techniques

1. In order to combat or counter the use of information and communications technologies for criminal purposes 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 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, without compromising the cyber security threat and confidentiality of the intelligence of each State Party.

2. For the purpose of investigating the offences involving the use of information and communications technologies 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, respect of fundamental human rights and freedoms 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.

Article 31 Return and disposal of assets

1. Property confiscated by a State Party pursuant to article 33 or 34 of this Convention shall be disposed of, including by return to its prior legitimate owners, pursuant to paragraph 3 of this article, by that State Party in accordance with the provisions of this Convention and its domestic law.

2. Each State Party shall adopt such legislative and other measures, in accordance with the fundamental principles of its domestic law, as may be necessary to enable its competent authorities to return confiscated property, when acting on the request made by another State Party, in accordance with this Convention, taking into account the rights of *bona fide* third parties.

3. In accordance paragraphs 1 and 2 of this Article, the requested State Party shall:

(a) In the case of countering the use of information and communications technologies as referred to in this Convention, when confiscation was executed in accordance with article ---- and on the basis of a final judgement in the requesting State Party, a requirement that can be waived by the requested State Party, return the confiscated property to the requesting State Party;

(b) In the case of proceeds of any other offence involving the use of information and communications technologies covered by this Convention, when the confiscation was executed in accordance with article --- of this Convention and on the basis of a final judgement in the requesting State Party, a requirement that can be waived by the requested State Party, return the confiscated property to the requesting State Party, when the requesting State Party reasonably establishes its prior ownership of such confiscated property to the requested State Party or when the requested State Party recognizes damage to the requesting State Party as a basis for returning the c confiscated property;

(c) In all other cases, give priority consideration to returning confiscated property to the requesting State Party, returning such property to its prior legitimate owners or compensating the victims of the crime.

4. Where appropriate, unless States Parties decide otherwise, the requested State Party may deduct reasonable

expenses incurred in investigations, prosecutions or judicial proceedings leading to the return or disposition of confiscated property pursuant to this article.

5. Where appropriate, States Parties may, in accordance with the domestic legislation, also give special consideration to concluding agreements or mutually acceptable arrangements, on a case-by-case basis, for the final disposal of confiscated property.