

## **United States Proposals for Criminalization, General Provisions, and Procedural Measures and Law Enforcement Chapters**

The United States submits to the Secretariat the following proposals of draft provisions for the criminalization, general provisions, and procedural measures and law enforcement chapters for consideration by Member States at the second negotiating session of the Ad Hoc Committee to elaborate a UN cybercrime treaty (AHC), taking into full consideration existing international instruments and efforts at the national, regional and international levels to combat cybercrime.

In brief, the United States proposes the **general provisions** define a select number of key terms with broad language that has been proven adaptable to changing technologies, incorporating existing UN terminology as appropriate. In addition, the United States proposes that the general provisions commit Member States to implement the convention in accordance with their broader obligations to respect human rights, fundamental freedoms, and sovereignty.

The United States proposes that the **criminalization** chapter require Member States to criminalize core cybercrimes through domestic legislation: crimes against computer systems or data (illegal access, illegal interception, data interference, system interference, misuse of devices) and select crimes for which the scope, speed, and scale of the offense are substantially enhanced by the use of a computer (computer-related fraud and forgery, child sexual abuse materials, and offenses related to infringements of copyright and related rights), as well as participation and attempt in such offenses, laundering of proceeds of cybercrime, and obstruction of justice.

The United States proposes that the **procedural measures and law enforcement** chapter enable Member States to collect and obtain electronic evidence for any type of crime. The specific procedural measures included below are expedited preservation of stored computer data, production orders, search and seizure of stored computer data, real-time collection of traffic data, and interception of content data. In addition, the United States has proposed that the AHC look to existing UN instruments for effective models for determining jurisdiction over offenses established under this convention, confiscation and seizure and return of confiscated assets, protection of witnesses, assistance to and protection of victims, and cooperation with law enforcement.

The United States appreciates this opportunity to provide potential text for the chapters to be discussed at the second session and welcomes feedback and further discussion.

# General Provisions

## USE OF TERMS

“**child**” means any individual under the age of 18.

“**child sexual abuse material**” shall mean any visual depiction or live transmission of (1) a child engaged in real or simulated sexually explicit conduct or (2) an adult engaged in real or simulated sexuality explicit conduct with a child intentionally included in the visual depiction or live transmission. It shall not be necessary for the child to be conscious or aware of, or able to appraise the nature of, such sexually explicit conduct. (Adapted from **Optional Protocol on the Sale of Children, Child Prostitution, and Child Pornography Article 2(c)**)

“**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 to perform such a function

“**computer system**” means any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.

“**confiscation**”, which includes forfeiture where applicable, shall mean the permanent deprivation of property by order of a court or other competent authority. (UNTOC Article 2(g))

“**cybercrimes**” mean offenses established in accordance with this Convention.

“**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. (UNTOC Article 2(f))

“**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 the criminalization of the laundering of proceeds of cybercrime article of this Convention. (UNTOC Article 2(h))

“**proceeds of crime**” shall mean any property derived from or obtained, directly or indirectly, through the commission of an offence. (UNTOC Article 2(e))

“**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. (UNTOC Article 2(d))

“**regional economic integration organization**” shall mean an organization constituted by sovereign States of a given region, to which its member States have transferred competence in respect of matters governed by this Convention and which has been duly authorized, in accordance with its internal procedures, to sign, ratify, accept, approve or accede to it; references to “States Parties” under this Convention shall apply to such organizations within the limits of their competence. (UNTOC Article 2(j))

**“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 a communication service or users of such service.

**“sexually explicit conduct”** includes at least the following real or simulated acts: a) sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, between children, or between an adult and a child; b) bestiality; c) masturbation; d) sadistic or masochistic abuse in a sexual context; or e) lascivious exhibition of the genitals or the pubic area of a child, whether clothed or nude.

**“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.

## **SCOPE OF APPLICATION**

This Convention shall apply, except as otherwise stated herein, to the prevention, investigation, and prosecution of the offences established in accordance with this Convention and collecting, obtaining, and sharing electronic evidence.

## **PROTECTION OF HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS AND THE RULE OF LAW**

1. States Parties shall carry out their obligations under this Convention with full respect for human rights and fundamental freedoms and the rule of law.
2. Nothing in this Convention shall be interpreted as affecting other rights and obligations of states and individuals under international law, including the Charter of the United Nations and international human rights law.
3. Any person who is taken into custody or regarding whom any other measures are taken or proceedings are carried out pursuant to this Convention shall enjoy all rights and guarantees in conformity with the law of the state in the territory of which that person is present and with relevant provisions of international human rights law, including the International Covenant on Civil and Political Rights.

## **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 or performance of functions that are reserved exclusively for the authorities of that other State by its domestic law.

**(UNTOC and UNCAC Article 4 )**

# Criminalization

## CRIMINALIZATION OF CYBERCRIMES

### **“illegal access”**

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, the access to the whole or any part of a computer system without right. A State 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.

### **“illegal interception”**

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

### **“data interference”**

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
2. A State Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

### **“system interference”**

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

### **“misuse of devices”**

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, 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 the preceding articles of this chapter

(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 the intent that it be used for the purpose of committing any of the offences established in the preceding articles of this chapter; 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 the preceding articles of this chapter. A State 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 the preceding articles of this chapter, such as for the authorized 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.

**“computer-related forgery”**

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, 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 of whether or not the data is directly readable or intelligible. A State Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

**“computer-related fraud”**

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

**“computer-related offenses involving child sexual abuse materials”**

1. Each State Party shall take the necessary legislative or other measures to ensure that the following conduct, when committed knowingly and through a computer system, is criminalized:

- a. producing child sexual abuse material;
- b. causing the live transmission of a child engaged in sexually explicit conduct;
- c. offering or making available child sexual abuse material;
- d. distributing or transmitting child sexual abuse material;
- e. procuring child sexual abuse material for oneself or for another person;
- f. possessing child sexual abuse material;
- g. knowingly obtaining access, through information and communication technologies, to child sexual abuse material or viewing the live transmission of a child engaged in sexually explicit conduct.

2. Each State Party shall take the necessary legislative or other measures to criminalize the knowing persuasion, inducement, enticement, or coercion, through information and communication technologies, of a child, or an individual believed to be a child, to engage in any illegal sexual activity. Each State Party shall take such necessary legislative or other measures to assure that its national law does not require a meeting in person between the individual and a child.

**“computer-related 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 the infringement of copyright, as defined under the law of that State 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 willfully, on a commercial scale and by means of a computer system.

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 Organizations (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 willfully, on a commercial scale and by means of a computer system.

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.

**“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.

**(UNCAC Article 27)**

## **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 the offences established in accordance with the criminalization articles 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.

**(UNTOC Article 10 and UNCAC Article 26)**

## **PROSECUTION, ADJUDICATION, and SANCTIONS**

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

2. Each State Party shall endeavor 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 the criminalization articles 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 the 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.

**(UNTOC Article 11)**

## **CRIMINALIZATION of the LAUNDERING OF PROCEEDS OF CYBERCRIME**

1. Each State Party shall adopt, in accordance with fundamental principles of its domestic law, such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally:

(a) (i) The conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her actions;

(ii) The concealment or disguise of the true nature, source, location, disposition, movement, or ownership of or rights with respect to property, knowing that such property is the proceeds of crime;

(b) Subject to the basic concepts of its legal system:

(i) The acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime;

(ii) Participation in, association with or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article.

2. For purposes of implementing or applying paragraph 1 of this article:

(a) Each State Party shall include as predicate offences the offences established in accordance with the criminalization articles of this Convention. In the case of States Parties whose legislation sets out a list of specific predicate offences, they shall, at a minimum, include the offences that are set forth in this convention;

(b) For the purposes of subparagraph (b), predicate offences shall include offences committed both within and outside the jurisdiction of the State Party in question. However, offences committed outside the jurisdiction of a State Party shall constitute predicate offences only when the relevant conduct is a criminal offence under the domestic law of the State where it is committed and would be a criminal offence under the domestic law of the State Party implementing or applying this article had it been committed there;

(c) Each State Party shall furnish copies of its laws that give effect to this article and of any subsequent changes to such laws or a description thereof to the Secretary-General of the United Nations;

(d) If required by fundamental principles of the domestic law of a State Party, it may be provided that the offences set forth in paragraph 1 of this article do not apply to the persons who committed the predicate offence;

(e) Knowledge, intent or purpose required as an element of an offence set forth in paragraph 1 of this article may be inferred from objective factual circumstances.

**(Adapted from UNTOC Article 6)**

## **CRIMINALIZATION OF OBSTRUCTION OF JUSTICE**

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally:

(a) The use of physical force, threats or intimidation or the promise, offering or giving of an undue advantage to induce false testimony or to interfere in the giving of testimony or the production of evidence in a proceeding in relation to the commission of offences covered by this Convention;

(b) The use of physical force, threats or intimidation to interfere with the exercise of official duties by a justice or law enforcement official in relation to the commission of offences covered by this Convention. Nothing in this subparagraph shall prejudice the rights of States Parties to have legislation that protects other categories of public officials.

(UNTOC Article 23)

# **Procedural Measures and Law Enforcement**

## **PROCEDURAL PROVISIONS**

### **“Scope of 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 section for the purpose of specific criminal investigations or proceedings.
2. Except as specifically provided otherwise in the article addressing interception of content data, each State Party shall apply the powers and procedures referred to in paragraph 1 of this article to:
  - (a) the criminal offences established in accordance with the criminalization chapter 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.

### **“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 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 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 State 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 State 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.

**“production order”**

1. Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium;

**“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) 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 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.

3. Each State 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.

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 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.

**“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 State 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 State 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 State 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 State 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.

**“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 State 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 State 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 State 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 associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3. Each State 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.

## **JURISDICTION**

1. Each State Party shall adopt such measures as may be necessary to establish its jurisdiction over 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.

2. Subject to the sovereignty article 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; 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 [money laundering article] of this Convention and is committed outside its territory with a view to the commission of an offence established in accordance with Article [money laundering article] of this Convention within its territory; or
- (d) the offence is committed against the State Party.

3. For the purposes of the extradition article 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 offences 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 State 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.

(UNCAC Article 42 and UNTOC Article 15)

## **CONFISCATION AND SEIZURE**

1. States Parties shall adopt, to the greatest extent possible within their domestic legal systems, such measures as may be necessary to enable confiscation of:

(a) Proceeds of crime derived from offences covered by this Convention or property the value of which corresponds to that of such proceeds;

(b) Property, equipment or other instrumentalities used in or destined for use in offences covered by this Convention.

2. States Parties shall adopt 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.

3. If 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.

4. If 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.

5. Income or other benefits derived from proceeds of crime, from property into which proceeds of crime have been transformed or converted or from property with which 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.

6. For the purposes of this article and article [international cooperation for purposes of confiscation] of this Convention, each State Party shall empower its courts or other competent authorities in order that bank, financial or commercial records be made available or be seized. States Parties shall not decline to act under the provisions of this paragraph on the ground of bank secrecy.

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

8. The provisions of this article shall not be construed to prejudice the rights of bona fide third parties.

9. 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.

(UNTOC Article 12)

## **DISPOSAL OF CONFISCATED PROCEEDS OF CRIME OR PROPERTY**

1. Proceeds of crime or property confiscated by a State Party pursuant to the article on confiscation and seizure and [any article on international cooperation for the purposes of confiscation] 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 [any article on international cooperation for the purposes of confiscation] 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 the article on confiscation and seizure and [any international cooperation for the purposes of confiscation] of this Convention, a State Party may, after due consideration has been given to compensation to victims, give special consideration to concluding agreements on 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 [any technical assistance article] of this Convention and to intergovernmental bodies specializing in the fight against cybercrime;
    - (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.
- (UNTOC Article 14)

## **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 relating to an offence covered by this Convention.

(UNTOC Article 22)

## **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.

(UNTOC Article 24 and UNCAC Article 32)

## **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.

(UNTOC Article 25)

## **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 offenses established by this convention:

(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 persons participating in offenses established by this convention;

(ii) Links, including international links, with other persons participating in offenses established by this convention;

(iii) Offences that persons participating in offenses established in this convention have committed or may commit;

(b) To provide factual, concrete help to competent authorities that may contribute to depriving [persons participating in offenses established by this convention] 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 the article on protection of witnesses 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.

(UNTOC Article 26)