Judge Stein Schjolberg

The Third Pillar for Cyberspace

An International Court or Tribunal for Cyberspace

Peace and Justice in Cyberspace

Chairman, High Level Experts Group (HLEG), ITU, Geneva, (2007-2008)
Chair, EastWest Institute (EWI) Cybercrime Legal Working Group, (2010-2013)
Chair, The Global Think Tank on Peace and Justice in Cyberspace (2013-)

stein.schjolberg@cybercrimelaw.net
www.cybercrimelaw.net

"There can be no peace without justice, no justice without law and no meaningful law without a Court to decide what is just and lawful under any given circumstances."

Benjamin B. Ferencz,
Former US Prosecutor

Draft United Nations Treaty on an International Criminal Court or Tribunal for Cyberspace
(10th Edition, June 2015)

by Judge Stein Schjolberg
www.cybercrimelaw.net

Introduction

Recalling the United Nations Convention against Transnational Organized Crime, adopted by General Assembly Resolution 55/25 in 2000, promoting international cooperation to more effectively prevent and combat transnational organized crime,

Recalling the United Nations Resolutions 55/63 in 2000 and 56/121 in 2001 on combating the criminal misuse of information technologies, in which it invited Member States to take into account measures to combat the criminal misuse of information technologies,

Recognizing that the free flow of information in cyberspace can promote economic and social development, education and democratic governance,

Noting that the rapid growth of the information and communication technology (ICTs) networks in cyberspace has created new opportunities for criminals in perpetrating crime, and to exploit online vulnerabilities and attack countries' critical information infrastructure,

Expressing concern that the technological developments in cyberspace have created new needs for cybersecurity measures in protecting against criminal activity and cyberthreats of critical concerns to the global society,

Noting that the developments of information and communication technologies in cyberspace has resulted in substantial increase in global cooperation and coordination, such that criminal activity may have a grave impact on all States,

Recognizing that differences in levels of information and communication technologies can diminish the effectiveness of international cooperation in combating the criminal activity in cyberspace, and recognizing the need for effective cybersecurity measures, in particular to developing countries, and the need for cooperation between States and the private sector,

Noting the necessity of preventing against criminal activities by adequate cybersecurity measures,

Recognizing with appreciation the work of the United Nations Office of Drugs and Crime (UNODC) in Vienna, and the outstanding workshops on computer crime and cybercrime at the United Nations Congresses on Crime Prevention and Criminal Justice in Bangkok in 2005 and Salvador, Brazil in 2010,

Underlining the need for a common understanding of cybersecurity and cybercrime among countries at all stages of economic development, and establish a global agreement or treaty at the United Nations level that includes solutions aimed at addressing the global challenges, that may promote peace and security in cyberspace,

including legal frameworks that are globally applicable and interoperable with the existing national and regional legislative measures,

Recognizing with appreciation the work of the World Summit on the Information Society (WSIS) in Tunis (2005).

Welcoming the work of Plenipotentiary Conference in 2006 organized by the International Telecommunication Union (ITU),

Recognizing with appreciation the work of the Global Cybersecurity Agenda (GCA) launched by the ITU in 2007 and the strategic proposals from the High Level Experts Group (HLEG), a global expert group of more than 100 experts, that delivered Recommendations in The Chairman´s Report and The Global Strategic Report in 2008, including strategies in the following five work areas: Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building, and International Cooperation,

Underlining the need for coordination and cooperation among States in the combat against cybercrime, and emphasize the role that can be played by the United Nations as described in the Salvador Declaration Article 42 (2010), adopted by the Commission on Crime Prevention and Criminal Justice and by the General Assembly in its resolution 65/230,

Welcoming the work of the open-ended Intergovernmental expert group on cybercrime, established by the UNODC in Vienna, that had its first meeting in Vienna, January 17-21, 2011, and the Second Meeting in Vienna, February 25-28, 2013.

Noting the work of international and regional organizations that have developed binding cybercrime instruments,

- The Council of Europe Convention on Cybercrime (2001)
- The League of Arab States Convention on Combating Information Technology Offences,
- The Commonwealth of Independent States Agreement on Cooperation in Combating Offences related to Computer Information,
- The Shanghai Cooperation Organization Agreement in the Field of International Information Security,
- African Union Convention on Cyber Security and Personal Data Protection (June 27, 2014)

and promoting dialogues between government and the private sector on security measures in cyberspace, since cyberthreats are global problems and need a global harmonization involving all stakeholders,

Underlining the need for strategies on the development of a treaty or a set of treaties for cybersecurity and cybercrime that may serve as a global model cybersecurity and cybercrime legislation that is applicable and interoperable with existing national and regional legislative measures,

Recalling the United Nations Human Rights Council Resolution of June 29, 2012, on the promotion, protection and enjoyment of human rights on the Internet (A/HRC/20/L.13):
"Affirms that the same rights that people have offline must also be protected online, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights."

Reaffirming the human rights and fundamental freedoms enshrined in the Universal Declaration of Human Rights and relevant international human rights treaties, including the International Covenant on Civil and Political Rights, and the International Covenant on Economic, Social and Cultural Rights,

Noting that the exercise of human rights, in particular the right of freedom of expression, on the Internet is an issue of increasing interest and importance as the rapid pace of technological development enables individuals all over the world to use new information and communications technologies,

Affirms that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one´s choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

A summary of the framework for the International Criminal Tribunal for Cyberspace may be as follows:

1. The judiciary is one of the three powers of any democratic state. Its mission is to guarantee the very existence of the Rule of Law and thus, to ensure the proper application of the law in an impartial, just, fair, and efficient manner. [1]

The International Criminal Tribunal for Cyberspace shall be a treaty based, fully independent international tribunal established to promote the rule of law similar or almost a parallel to a Supreme Court.

The International Criminal Tribunal for Cyberspace[2] *is established by the United Nations General Assembly, or by the United Nations Security Council acting under Chapter VII of the Charter of the United Nations. The purpose is to prevent serious and organized global cybercrime, protect the peace and ensure that the most serious international crimes in cyberspace do not go unpunished.*

2. Any intentional electronic communications surveillance in investigations of criminal cases across jurisdictional boundaries needs the consent of the International Criminal Tribunal for Cyberspace or the Prosecutors Office, whenever there is

---

[1] See The Magna Carta of Judges (Fundamental Principles) Article 1, adopted by the Consultative Council of European Judges in 2010.

[2] The Statute of the International Criminal Tribunal for The Former Yugoslavia has been used as a Model Statute. Article 19 on the Electronic Communication Surveillance is based on models in the Norwegian Criminal Procedure Act Chapter 16a, and in the US Foreign Intelligence Surveillance Act (FISA), as required in 50 USC § 1805 – Issuance of order, that does not apply outside the United States.

probable cause to believe that anybody is suspected of having committed or attempt to commit cyberattacks and other cybercrimes of the most serious global concern,

3. A permanent appointed defense attorney shall be present at the Court hearings and be a protector of the basic legal and procedural rights of the offender.

4. The Prosecutor, as a separate organ of the International Criminal Tribunal for Cyberspace, shall be responsible for the investigation and prosecution of cyberattacks and other cybercrimes of the most serious global concern.

The Prosecutors Office shall act independently of the Security Council, of any State, or any international organization, or of other organs of the International Criminal Tribunal for Cyberspace.

5. The Prosecutors Office shall have the power to seek assistance in the investigation by global law enforcements coordinated by INTERPOL, and the global private sector.

6. The principle sources for the protection of individual rights, the Universal Declaration on Human Rights, the International Covenant on Civil and Political Rights, and the International Covenant on Economic, Social and Cultural Rights, are fundamental rights that support the right of every person to exercise the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any medium regardless of frontiers.

(The International Criminal Tribunal for Cyberspace is hereafter referred to as "the International Tribunal") shall function in accordance with the provisions of the present Statute)

Article 1

Competence of the International Tribunal

The International Tribunal shall have the power to prosecute persons responsible for the most serious cyberattacks and cybercrimes of global concern, in accordance with the provisions of the present Statute.

Article 2

Global cyberattacks against critical communications and information infrastructures

The International Tribunal shall have the power to prosecute persons committing or ordering to be committed the most serious cyberattacks of global concern as violations of international cybercrime law, namely the following acts committed willfully against computer systems, information systems, data, information or other property protected under the relevant international criminal law;

Whoever, by destroying, damaging, or rendering unusable critical communications and information infrastructures, causes substantial and comprehensive disturbance to the national security, civil defense, public administration and services, public health or safety, or banking and financial services.

International cybercrime may under any circumstances be considered as most serious cybercrime of global concern, whenever the cybercrime involves 10 countries and more, and losses of more than 100 million US dollars, and more than 500 000 victims.

Article 3

Other cybercrime of the most serious global concern

The International Tribunal shall have the power to prosecute persons committing or ordering to be committed the most serious cybercrimes of global concern as violations of international cybercrime law, namely the following acts committed willfully against computer systems, information systems, data, information or other property protected under the relevant international criminal law;

a) illegal access

b) illegal interception

c) data interference

d) system interference

e) misuse of devices

f) forgery

g) fraud

h) offences related to child pornography

Article 4

Social networks and identity theft

The International Tribunal shall have the power to prosecute persons committing or ordering to be committed of the most serious cybercrime of global concern as violations of international cybercrime law, namely the following acts committed willfully against computer systems, information systems, data, social networks, information or other property protected under the relevant international criminal law;

a) identity theft

b) other most serious crimes on social networks of global concern

Article 5

Preparatory acts of provisions in the global statute on cyberattacks and cybercrime

The International Tribunal shall have the power to prosecute persons committing or ordering to be committed the most serious violations of international cybercrime law, namely the following acts committed willfully against computer systems, information systems, data, information or other property protected under the relevant international criminal law;

the preparation of an information or communication technology tool or condition, that is especially suitable to commit a cybercrime of the most serious global concern as referred to in Article 2-4.

Article 6

Personal jurisdiction

The International Tribunal shall have jurisdiction over natural persons pursuant to the provisions of the present Statute.

Article 7

Individual criminal responsibility

1. A person who planned, instigated, ordered, committed or otherwise aided and abetted in the planning, preparation or execution of a crime referred to in articles 2 to 5 of the present Statute, shall be individually responsible for the crime.

2. The official position of any accused person, whether as head of state or Government or as a responsible Government official, shall not relieve such person of criminal responsibility nor mitigate punishment.

3. The fact that any of the acts referred to in articles 2 to 5 of the present Statute was committed by a subordinate does not relieve his superior of criminal responsibility if he knew or had reason to know that the subordinate was about to commit such acts or had done so and the superior failed to take the necessary and reasonable measures to prevent such acts or to punish the perpetrators thereof.

4. The fact that an accused person acted pursuant to an order of a Government or of a superior shall not relieve him of criminal responsibility, but may be considered in mitigation of punishment if the International Tribunal determines that justice so requires.

Article 8
Jurisdiction
1. The jurisdiction of the Tribunal shall be limited to the most serious cybercrimes of concern to the international community as a whole. The Tribunal has jurisdiction in accordance with this Statute with respect to the crimes included in Articles 2-5.

2. The Tribunal shall exercise jurisdiction over additional cybercrimes according to future decisions of the Statute by the Security Council.

Article 9

Concurrent jurisdiction

The International Tribunal shall have primacy over national courts. At any stage of the procedure, the International Tribunal may formally request national courts to defer to the competence of the International Tribunal in accordance with the present Statute and Rules of Procedure and Evidence of the International Tribunal.

Article 10

Non-bis-in-idem

1. No person shall be tried before a national court for acts constituting serious violations of international cybercrime law committed under the present Statute, for which he or she already have been tried by the International Tribunal.

2. A person who has been tried by a national court for acts constituting serious violations of international cybercrime law may be subsequently tried by the International Tribunal only if:

a) the act for which he or she was tried was characterized as an ordinary crime; or

b) the national court proceedings were not impartial or independent, were designed to shield the accused from international responsibility, or the case was not diligently prosecuted.

3. In considering the penalty to be imposed on a person convicted of a crime under the present Statute, the International Tribunal shall take into account the extent to which any penalty imposed by a national court on the same person for the same act has already been served.

Article 11

Organization of the International Tribunal

The International Tribunal shall consist of the following organs:

a) the Chambers, comprising three Trial Chambers and an Appeals Chamber;

b) the Prosecutor; and

c) a Registry, serving both the Chambers and the Prosecutor.

Article 12

Composition of the Chambers

1. The Chambers shall be composed of a maximum of sixteen permanent independent judges, no two of whom may be nationals of the same State, and a maximum at any one time of twelve *ad litem* judges appointed in accordance with article 13 *ter,* paragraph 2, of the Statute, no two of whom may be nationals of the same State.

Five of the judges should be appointed from each of the five veto-wielding permanent members of the United Nations Security Council – China, France, Russia, the United Kingdom, and the United States.

2. A maximum at any one time of three permanent judges and six *ad item* judges shall be members of each Trial Chamber. Each Trial Chamber to which *ad litem* judges are assigned may be divided into sections of three judges each, composed of both permanent and *ad litem,* except in the circumstances specified in paragraph 5 below. A section of a Trial Chamber shall have the same powers and responsibilities as a Trial Chamber under the Statute and shall render judgment in accordance with the same rules.

3. Seven of the permanent judges shall be members of the Appeals Chamber. The Appeals Chamber shall, for each appeal, be composed of five of its members.

4. A person who for the purposes of membership of the Chambers of the International Tribunal could be regarded as a national of more than one State shall be deemed to be

a national of the State in which that person ordinarily exercises civil and political rights.

5. The Secretary-General may, at the request of the President of the International Tribunal appoint, from among the *ad litem* judges elected in accordance with Article 13 *ter*, reserve judges to be present at each stage of a trial to which they have been appointed and to replace a judge if that judge is unable to continue sitting.

6. Without prejudice to paragraph 2 above, in the event that exceptional circumstances require for a permanent judge in a section of a Trial Chamber to be replaced resulting in a section solely comprised of *ad item* judges, that section may continue to hear the case, notwithstanding that its composition no longer includes a permanent judge.

Article 13

Qualifications of judges

The permanent and *ad litem* judges shall be persons of high moral character, impartiality and integrity who possess the qualifications required in their respective countries for appointment to the highest judicial offices. In the overall composition of the Chambers and sections of the Trial Chambers, due account shall be taken of the experience of the judges in criminal law and international law.

Article 13 *bis*

Election of permanent judges

Article 13 *ter*

Election and appointment of *ad litem* judges

Article 13 *quater*

Status of *ad litem* judges

Article 14

Officers and members of the Chambers

1. The permanent judges of the International Tribunal shall elect a President from amongst their number.

2. The President of the International Tribunal shall be a member of the Appeals Chamber and shall preside over its proceedings.

3. After consultation with the permanent judges of the International Tribunal, the President shall assign four of the permanent judges elected or appointed in accordance with article 13 *bis* of the Statute to the Appeals Chamber and eleven to the Trial Chambers. Notwithstanding the provisions of article 12, paragraph 1, and article 12, paragraph 3, the President may assign to the Appeals Chamber up to four additional permanent judges serving in the Trial Chambers, on the completion of the cases to which each judge is assigned. The term of office of each judge redeployed to the Appeals Chamber shall be the same as the term of office of the judges serving in the Appeals Chamber.

4. After consultation with the permanent judges of the International Tribunal, the President shall assign such *ad litem* judges as may from time to time be appointed to serve in the International Tribunal to the Trial Chambers.

5. A judge shall serve only in the Chamber to which he or she was assigned.

6. The permanent judges of each Trial Chamber shall elect a President Judge from amongst their number, who shall oversee the work of the Trial Chamber as a whole.

Article 15

Rules of procedure and evidence

The judges of the International Tribunal shall adopt rules of procedure and evidence for the conduct of the pre-trial phase of the proceedings, trials and appeals, the admission of evidence, the protection of victims and witnesses and other appropriate matters.

Article 16

The Prosecutor

1.The Prosecutor shall be responsible for the investigation and prosecution of persons responsible for the most serious cyberattacks and cybercrimes of global concern.

2. The prosecutor shall act independently as a separate organ of the International Tribunal. He or she shall not seek or receive instructions from any Government or from any other source.

3. The Office of the Prosecutor shall be composed of a Prosecutor and such other qualified staff as may be required.

4. The Prosecutor shall be appointed by the Security Council on nomination by the Secretary-General. He or she shall be of high moral character and possess the highest level of competence and experience in the conduct of investigations and prosecutions of criminal cases. The Prosecutor shall serve for a four-year term and be eligible for reappointment. The terms and conditions of service of the Prosecutor shall be those of an Under-Secretary-General of the United Nations.

5. An Advisory Board for the Office of the Prosecutor shall be appointed from each of the five veto-wielding permanent members of the United Nations Security Council – China, France, Russia, the United Kingdom, and the United States.

6. The Advisory Board shall have the power of each to veto any indictments before the International Tribunal. Abstention is not regarded as a veto.

Procedural matters or avoid discussions of an issue shall not be subject to a veto. A veto cannot be used to avoid any decision by the Prosecutor of opening of an investigation.

7. The Staff of the Office of the Prosecutor shall be appointed by the Secretary-General, on the recommendation of the Prosecutor.

Article 17

The Registry

1. The Registry shall be responsible for the administration and serving of the International Tribunal.

2. The Registry shall consist of a Registrar and such other staff as may be required.

3. The Registrar shall be appointed by the Secretary-General, after consultation with the President of the International Tribunal. He or she shall serve for a four-year term and be eligible for reappointment. The terms and conditions of service of the Registrar shall be those of an Assistant Secretary-General of the United Nations.

4. The staff of the Registry shall be appointed by the Secretary-General, on the recommendation of the Registrar.

Article 18

Investigation and preparation of indictment

1. The Prosecutor shall initiate investigations ex-officio or on the basis of information obtained from any source, particularly from Governments, United Nations organs, intergovernmental and non-governmental organizations. The Prosecutor shall assess the information received or obtained and decide whether there is sufficient basis to proceed.

2. The Prosecutors Office shall have the power to collect evidence and to conduct all kinds of cyber investigation, and question suspects, victims and all other involved as parts and witnesses in the crime. In carrying out these tasks, the Prosecutor may, as appropriate, seek the assistance of the State authorities concerned.

3. The Prosecutors Office shall have the power to seek assistance in the investigation by global law enforcements coordinated by INTERPOL.

4. The Prosecutors Office shall have the power to seek assistance in the investigation by a Global Virtual Taskforce established by key stakeholders in the global information and communications technology industry, global private sector, non-governmental organizations, and the global law enforcement coordinated by INTERPOL.

5. The Prosecutor may request a judge of the Trial Chamber, to issue such orders or warrants for the electronic communications surveillance, arrest, detention, surrender or transfer of persons, and any other orders as may be required for the conduct of the investigation or trial.

6. The Prosecutor shall be pursuing the proceeds of crime and apply for a Sequestration Order from the judge of the Trial Chamber. A Confiscation Order may subsequently be sought following conviction.

7. Upon a determination that a *prima facie* case exists, The Prosecutor shall prepare an indictment containing a concise statement of the facts and the crime or crimes with which the accused is charged under the Statute. The indictment shall be transmitted to a judge of the Trial Chamber.

Article 19

Electronic Communications Surveillance

Any intentional electronic communications surveillance in investigations of criminal cases across jurisdictional boundaries needs the consent of the International Tribunal or the Prosecutors Office.

1. The Court may make an order permitting the Prosecutor to carry out electronic communications surveillance whenever there is probable cause to believe that anybody is suspected of having committed or attempt to commit:

- a global cyberattack against critical communications and information infrastructures of a country (Article 2),
- other cybercrimes of the most serious global concern (Article 3)

2. The Prosecutor shall present the request for an electronic communications surveillance order before the judge. The request may be approved or denied, or the judge may require the request to be modified before being accepted. The request may also only partially be approved by the judge.

3. The surveillance hearing is not open to the public, and the court hears evidences solely by the Prosecutor.

A permanent appointed defense attorney shall be present at the Court hearing and be a protector of the basic legal and procedural rights of the offender.

The court decision shall not be published. All persons shall maintain secrecy concerning any application or decision relating to electronic communication control in any case, and concerning any information derived from such control.

4. The Prosecutor may if an emergency situation exists, authorize an emergency order for an electronic communications surveillance of anybody under the same conditions as stated in No.1 for a period of until 72 hours. Everybody involved in the process of electronic communications surveillance shall keep all information secret, except as evidence in a court hearing,

5. Judicial authorization is required within 72 hours after the electronic communications surveillance is authorized by the Prosecutor.

6. Any Court order for electronic communications surveillance may be approved for the period necessary to achieve its purpose, not exceeding 90 days for each court approval.

Extension of an order issued under this Article may be granted on the same basis as an original order upon an application for an extension and new findings made in the same manner as regarded for an original order.

7. An order approving an electronic surveillance under this article in circumstances where the nature and country and location each of the facilities or places at which the surveillance will be directed is unknown, shall direct the applicant to provide notice to the court within ten days after the date on which surveillance begins to be directed at any new facility or place.

8. The Court decision on a surveillance warrant may be appealed by the Prosecutor to the Appeal Chamber.

Article 19 bis

Electronic Communications Surveillance – specification of court orders

A Court order approving an electronic surveillance shall specify:

1. the identity or a description of the specific target of the electronic surveillance identified or described in the application,

2. the nature, country and location of each of the facilities or places at which the electronic surveillance will be directed, if known,

3. the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance,

4. the means by which the electronic surveillance will be affected,

5. the period of time during which the electronic surveillance is approved.

Article 20

Review of the indictment

The judge of the Trial Chamber to whom the indictment has been transmitted shall review it. If satisfied that a *prima facie* case has been established by the Prosecutor, he or she shall confirm the indictment. If not so satisfied, the indictment shall be dismissed.

Article 21

Commencement and conduct of trial proceedings

1. The Trial Chambers shall ensure that a trial is fair and expeditious and that proceedings are conducted in accordance with the rules of procedure and evidence, with full respect for the rights of the accused and due regard for the protection of victims and witnesses.

2. A person against whom an indictment has been confirmed shall, pursuant to an order or an arrest warrant of the International Tribunal, be taken into custody, immediately informed of the charges against him and transferred to the International Tribunal.

3. The Trial Chamber shall read the indictment, satisfy itself that the rights of the accused are respected, confirm that the accused understands the indictment, and instruct the accused to enter a plea. The Trial Chamber shall then set the date for a trial.

4. The hearings shall be public unless the Trial Chamber decides to close the proceedings in accordance with its rules of procedure and evidence.

Article 22

Rights of the accused

1. All persons shall be equal before the International Tribunal.

2. In the determination of charges against him, the accused shall be entitled to a fair and public hearing, subject to article 23 of the Statute.

3. The accused shall be presumed innocent until proved guilty according to the provisions of the present Statute.

4. In the determination of any charge against the accused pursuant to the present Statute, the accused shall be entitled to the following minimum guarantees, in full equality:

(a) to be informed promptly and in detail in a language which he or she understands of the nature and cause of the charge against him;

(b to have adequate time and facilities for the preparation of his or her defense and to communicate with counsel of his or her own choosing;

(c) to be tried without undue delay;

(d) to be tried in his or her presence, and to defend themselves in person or through legal assistance of his or her own choosing, if he or she does not have legal assistance, of this right; and to have legal assistance assigned to him or her, in any case where the interests of justice so require, and without payment by him or her in any such case if he or she does not have sufficient means to pay for it;

(e) to examine, or have examined, the witnesses against him or her and to obtain the attendance and examination of witnesses on his or her behalf under the same conditions as witnesses against him or she;

(f) to have the free assistance of an interpreter if he or she cannot understand or speak the language used in the International Tribunal;

(g) not to be compelled to testify against himself or herself or to confess guilt.

Article 23

Protection of victims and witnesses

The International Tribunal shall provide in its rules of procedure and evidence for the protection of victims and witnesses. Such protection measures shall include, but shall not be limited to, the conduct of camera proceedings and the protection of the victim`s identity.

A witness may be entitled to enter a Witness Protection Program to ensure their availability to provide evidence at a trial.

Article 24

Judgment

1. The Trial Chambers shall pronounce judgments and impose sentences and penalties on persons convicted of the most serious cyberattakcs and cybercrimes of global concern.

2. The judgment shall be rendered by a majority of the judges of the Trial Chamber, and shall be delivered by the Trial Chamber in public. It shall be accompanied by a reasoned opinion in writing, to which separate or dissenting opinions may be appended.

Article 25

Penalties

1. The penalty imposed by the Trial Chamber shall be limited to imprisonment.

2. In imposing the sentences, the Trial Chambers should take into account such factors as the gravity of the offence and the individual circumstance of the convicted person.

3. In addition to imprisonment, the Trial Chambers may order the return of any property and proceeds acquired by criminal conduct, including by means of duress, to their rightful owners.

Article 26

Appellate proceedings

1. The Appeals Chamber shall hear appeals from persons convicted by the Trial Chambers or from the Prosecutor on the following grounds:

(a) an error on a question of law invalidating the decision; or

(b) an error of fact which has occasioned a miscarriage of justice

2. The Appeals Chamber may affirm, reverse or revise the decisions taken by the Trial Chambers.

Article 27

Review proceedings

Where a new fact has been discovered which was not known at the time of the proceedings before the Trial Chambers or the Appeals Chamber and which could have been a decisive factor in reaching the decision, the convicted person or the Prosecutor may submit to the International Tribunal an application for review of the judgment.

Article 28

Enforcement of sentences

Imprisonment shall be served in a State designated by the International Tribunal from a list of States that have indicated to the Security Council their willingness to accept convicted persons. Such imprisonment shall be in accordance with the applicable law of the State concerned, subject to the supervision of the International Tribunal.

Article 29

Pardon or commutation of sentences

If, pursuant to the applicable law of the State in which the convicted person is imprisoned, he or she is eligible for pardon or commutation of sentence, the State concerned shall notify the International Tribunal accordingly. The President of the International Tribunal, in consultation with the judges, shall decide the matter on the basis of the interests of justice and the general principles of law.

Article 30

Co-operation and judicial assistance

1. States shall co-operate with the International Tribunal in the investigation and prosecution of persons accused of committing the most serious cyberattacks and cybercrimes of global concern.

2. States shall comply without undue delay with any request for assistance or an order issued by a Trial Chamber, including, but not limited to:

(a) the identification and locations of persons;

(b) the taking of testimony and the production of evidence;

(c) the service of documents;

(d) the arrest or detention of persons;

(e) the surrender or the transfer of the accused to the International Tribunal.

Article 31

The status, privileges and immunities of the International Tribunal

1. The Convention on the Privileges and Immunities of the United Nations of 13 February 1946 shall apply to the International Tribunal, the judges, the Prosecutor and his or her staff, and the Registrar and his or her staff.

2. The judges, the Prosecutor and the Registrar shall enjoy the privileges and immunities, exemptions and facilities accorded to diplomatic envoys, in accordance with international law.

3. The staff of the Prosecutor and of the Registrar shall enjoy the privileges and immunity accorded to officials of the United Nations under articles V and VII of the Convention referred to in paragraph 1 of this article.

4. Other persons, including the accused, required at the seat of the International Tribunal shall be accorded such treatment as is necessary for the proper functioning of the International Tribunal.

Article 32

Seat of the International Tribunal

The International Tribunal shall have its seat at a location according to the Security Council decision.

Article 33

Expenses of the International Tribunal

The expenses of the International Tribunal shall be borne by the regular budget of the United Nations in accordance with Article 17 of the Charter of the United Nations.

Article 34

Working languages

The working languages of the International Tribunal shall be English and French.

Article 35

Annual report

The President of the International Tribunal shall submit an annual report of the International Tribunal to the Security Council and to the General Assembly.