Peace and Justice in Cyberspace

Potential new global legal mechanisms against global cyberattacks and other global cybercrimes

An International Criminal Tribunal for Cyberspace (ICTC)
International cybercrime law
Prosecution for the Tribunal
Police investigation for the Tribunal

by

Judge Stein Schjolberg

A Background Paper

for

EastWest Institute (EWI) Worldwide Cybersecurity Summit
Special Interest Seminar:
Harmonizing of Legal Frameworks for Cyberspace

New Dehli, India
October 30-31, 2012

Stein Schjolberg
Judge
Norway
Chairman, High Level Experts Group (HLEG), ITU, Geneva, (2007-2008)
Chair, EastWest Institute (EWI) Cybercrime Legal Working Group, (2010-)

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

"A discussion of digital risks should be on the agenda of board meetings everywhere as cyber attacks become more frequent, more creative and more disruptive. Cybercrime is an international business aided by those countries without the legislation framework to tackle it.
If we are serious about combating cybercrime, we need to increase international communication and collaboration between governments and businesses, and move towards uniform global regulation."

Lord Levene, Chairman of Lloyds

An International Criminal Tribunal for Cyberspace (ICTC)

By Judge Stein Schjolberg

Norway

"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, Prosecutor at The Nuremberg War Crimes Tribunal

(1920-)

1. Introduction

In the prospect of an international criminal court lies the promise of universal justice.[1] Without an international court or tribunal for dealing with the most serious cybercrimes of global concern, many serious cyberattacks will go unpunished.

The most serious global cyberattacks in the recent year, have revealed that almost nobody is investigated and prosecuted, and nobody has been sentenced for those acts. Such acts need to be included in a global treaty or a set of treaties, and investigated and prosecuted before an international criminal court or tribunal.

Cyberspace, as the fifth common space, after land, sea, air and outer space, is in great need for coordination, cooperation and legal measures among all nations. It is necessary to make the international community aware of the need for a global response to the urgent and increasing cyberthreats. Peace, justice and security in cyberspace should be protected by international law through a treaty or a set of treaties under the United Nations.

The progressive developments of global cyberattacks, such as massive and coordinated attacks against critical information infrastructures of sovereign States, must necessitate an urgent response for a global treaty.

Working Groups

The International Telecommunication Union (ITU) launched in May 2007 the Global Cybercrime Agenda (GCA) for a framework where the international response to growing challenges on cybersecurity could be coordinated. In order to assist the ITU in developing strategic proposal, a global High-Level Experts Group (HLEG) was established in October

[1] Kofi Annan, former UN Secretary-General

2007. This global experts group of almost 100 persons from around the world delivered the Chairmans Report and the Global Strategic Report in 2008 with recommendations on cybersecurity and cyber crime legislations.

Four main Working Groups have been established in 2010 in order to make recommendations for new international legal responses to cybercrime.

The United Nations has initiated a comprehensive study of the problem of cybercrime. The 12th United Nations Congress on Criminal Prevention and Criminal Justice in Salvador, Brazil, April 2010, recommended in the Salvador Declaration Article 42 to invite the UN Commission on Crime Prevention and Criminal Justice to convene an open-ended intergovernmental expert group to conduct a comprehensive study on the problem of cybercrime as well as the response to it. The recommendation was adopted by the Commission, and by the United Nations General Assembly in its resolution 65/230. This comprehensive study is to examine the topics *"with a view to examening options to strengthen existing and to propose new national and international legal or other responses to cybercrime."*

The Expert Group had its first meeting in Vienna on January 17-21, 2011.[2]

The EastWest Institute (EWI)[3] has on June 27, 2010, established a Cybercrime Legal Working Group,[4] in order to advance consideration of a treaty or a set of treaties on cybersecurity and cybercrime. The members are independent non-governmental global experts on cybersecurity and cybercrime. The Working Group shall develop recommendations for potential new legal mechanisms on combatting cybercrime and cyberattacks, and *"develop a consensus-building set of proposals related to international law."* The group had its first meeting in Brussels on March 1-2, 2010. It is necessary to include the global private sector and industry in the process of establishing a global treaty or a set of treaties on cybersecurity and cybercrime.[5]

United States and the European Union have established a Working Group on Cybersecurity and Cybercrime at the EU-US Summit in November 2010.[6] The group is

---

[2] See www.unodc.org

[3] See www.ewi.info

[4] This Working Group was established by a recommendation from judge Stein Schjolberg, Norway, in a letter of May 27, 2010, to John Edwin Mroz, President and CEO of EWI. The Working Group is a partnership with Cybercrimedata, Norway.

[5] UNODC had invited private sector companies to their meeting in Vienna, January 2011, but only one company attended.

[6] See www.europa.eu and MEMO/10/597

tasked with developing collaborative approaches to a wide range of cybersecurity and cybercrime issues. Among the efforts is *"advancing the Council of Europe Convention on Cybercrime, including a programme to expand accession by all EU Member States, and collaboration to assist states outside the region in meeting its standards and become parties."* The group had its first meeting in February 2011. EU has added a part covering large-scale attacks, which is an emerging trend and not fully covered in the Convention.[7]

The Commonwealth has at the Meeting for Law Ministers and Attorney-Generals from 44 countries in Sydney, July 2011,[8] recommended that the Commonwealth Secretariat established a multidisciplinary Working Group of experts. The purpose of this Working Group is to *"review the practical implications of cybercrime in the Commonwealth and identify the most effective means of international co-operation and enforcement, taking in to account, amongst others, the Council of Europe Convention on Cybercrime, without duplicating the work of other international bodies."* This Working Group should also identify *"the best practice, educational material and training programme for investigators, prosecutors and judicial officers."*

2. Substantive criminal law in the Statute for the International Criminal Tribunal for Cyberspace (ICTC)

2.1. Principles in substantive criminal law for cyberspace

The 2001 Council of Europe Convention on Cybercrime is a historic milestone in the combat against cyber crime, and entered into force on July 1, 2004. The total number of signatures not followed by ratifications are 12, and 35 States have ratified the Convention.[9] In Europe, Russia has not signed the Convention and has made a statement that they will not accept all Articles of the Convention.

By ratifying or acceding to the Convention, the States agree to ensure that their domestic laws criminalize the conducts described in the substantive criminal law section.

Considering the Council of Europe's Convention on Cybercrime as an example of legal measures realized as a regional initiative, European countries should complete its ratification. Other countries should consider the possibility of acceding to the Convention,

[7] Cecilia Malmstrom, Member of the EU Commission, in a speech on April 13, 2011.
[8] See www.thecommonwealth.org
[9] See www.conventions.coe.int (June 2012)

or use the Convention as a guideline, or use it as a reference for developing their internal legislation, by implementing the standards and principles it contains, in accordance with their own legal system and practice. It is very important to implement at least Articles 2-9 in the substantive criminal law section.

But the Convention is based on criminal cyber conducts in the late 1990s. New methods of conducts in cyberspace with criminal intent must be covered by criminal law, such as phishing, botnets, spam, identity theft, crime in virtual worlds, terrorist use of Internet, and massive and coordinated cyber attacks against information infrastrutures. Many countries have adopted or are preparing for new laws covering some of those conducts. In addition, the terminology included in the Convention is a 1990s terminology, and is not necessarily suitable for the 2010s.

Professor Marco Gercke, Germany,[10] has in his paper: *"10 years Convention on Cybercrime"* made a following conclusion why the Convention does not play an important role beyond the borders of Europe:

"The list of reasons why the Convention did not succeed at global level is complex. It starts with a missing involvement of developing countries in the drafting process, a more demanding accession procedure compared to UN Conventions, a lack of updates in response to trends, the absence of regulations for electronic evidence and liability of Internet Service Provider (ISP), missing field offices outside Europe and maybe most importantly a lack of supporting capacity building that is especially relevant for developing countries."

Provisions on attempt, aiding or abetting should be enacted and implemented in accordance with the individual countries own legal system and practice and need not necessarily be included in a convention. Similar approach should be taken with regard to corporate liability, and punishable sanctions and measures for criminal offences.

In order to establish criminal offences for the protection of information and communication in Cyberspace, provisions must be enacted with as much clarity and specificity as possible, and not rely on vague interpretations in the existing laws. When cybercrime laws are adopted, perpetrators will then be convicted for their explicit acts and not by existing provisions stretched in the interpretations, or by provisions enacted for other purposes covering only incidental or peripheral acts.

[10] See Marco Gercke, Computer Law Review International, Issue 5 15. October 2011, page 129-160, see cr-international.com. See also his website www.cybercrime.de

One of the most important purposes in criminal legislation is the prevention of criminal offenses. A potential perpetrator must also in cyberspace have a clear warning with adequate foreseeability that certain offences are not tolerated. And when criminal offences occur, perpetrators must be convicted for the crime explicitly done, satisfactorily efficient in order to deter him or her, and others from such crime. These basic principles are also valid for cybercrimes and global cyberattacks.

2.2. The most serious violations of international cybercrime law

Legal definitions should be enacted and implemented in cybercrime legislation in accordance with the legal system and practise in the individual country. Common law countries have a legal tradition of including definitions in the legal text itself, while civil law countries prefer to exclude such definitions. Civil law countries have a tradition of legal interpretations of the text in the individual provision, in accordance with the accepted current interpretations.

Each Party to the Treaty must, for he purpose of the Treaty, be able to enact and implement legal definitions in accordance with its legal system and practise.

Explanatory comments on illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud and offences related to child pornography are available in the explanatory report of the Council of Europe Cybercrime Convention.[11]

2.2.1. Massive and coordinated global cyberattacks against communications and information infrastructures

Several governments and vital private institutions in the global information and financial infrastructures have been targets by global cyberattacks in the recent year.

The UK government was a target when cyberattacks were launched on Whitehall and defence industry last year.[12] Both the Canadian and South Korean governments have recently suffered global cyberattacks. In Australia the computer system in the Parliament has been accessed in March 2011 by global cyberattacks, and the Prime Minister and several ministers computers may have been compromised.

[11] See www.conventions.coe.int

[12] Foreign Secretary William Hague at an international security summit in Munich, Germany, February 7, 2011.

Also regional organizations, such as the European Union, has been targeted by cyberattacks. The Commission of the European Union and the EU External Action service became in the recent year victims of a large scale cyberattack that severely affected the e-mail systems.[13]

The French Government has experienced cyberattacks on the countryś finance, economy and unemployment Ministry in 2010-2011 over a two months periode before the G20 Meeting. France had the Presidency of the meeting and a leakage of high level information may had threaten the economic and national security of the concerned countries.

In the private industry, the UK and US stock exchanges have been targets of global cyberattacks, aimed to spread panic in leading global financial markets. The parent company of NASDAQ in New York has been one of the victims, and in conjunction with the WikiLeaks, global cyberattacks have been launched against Visa, MasterCard, and PayPal.

These are only a few examples that some countries critical information infrastructures are under attack. The cyberattacks on sensitive national information infrastructure are rapidly emerging as one of a country´s most alarming national security threats, and are becoming a most serious cybercrime of global concern.

Cyberattacks may also be covered as an ordinary conduct of articles on data interference or system interference. But some countries have choosen to establish the aggravated circumstances or qualified acts as a separate provision, based on requirements such as " substantial and comprehensive disturbance to national security" or similar terms. The recent development of the most serious cyberattacks on critical government and private industry information infrastructure, have also revealed a necessity for implementing separate provisions on the intentional substantial and comprehensive disturbance to critical national infrastructures and security, combined with very severe imprisonments.

Critical communication and information infrastructures of a sovereign State are very vulnerable, both for the governmental institutions and the private industry, and a cyberattack may have the most serious and destructive consequences.

With this background intentional global cyberattacks against critical national infrastructures and security should be included in the preparation of a draft treaty for a global Statute since it have not yet been regulated by international law, or in regard to which the law has not yet been sufficiently developed in the practices of States.[14] Based on the

[13] Cecilia Malmstrom, Member of the EU Commission, in a speech on April 13, 2011.

[14] See the Statute of the International Law Commission, Article 15, www.un.org/law/ilc/

HLEG recommendations, laws against the massive and coordinated cyberattacks against critical communications and information infrastructures should be implemented. Such global or transcontinental attacks are rapidly increasing and need to be covered by a global Treaty.

It is therefore important that all countries implements legislations necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, whoever by destroying, damaging, or rendering unusable critical communications and information infrastructures, causes substantial and comprehensive disturbance to the national security, civil defence, public administration and services, public health or safety, or banking and financial services.

Such content may in fact be a qualified or agrevated circumstances in Articles on data interference or system interference. The differences is based on a requirement of the intent also covering "substantial and comprehensive disturbance to the national security, civil defence, public administration and services, public health or safety, or banking and financial services." This is ordinary fulfilled by a general and overall judgement of several elements such as the duration, dimension, effect of the disturbance.

2.2.2. New assets or interests developed on cyberspace that may need the protection of substantive criminal law

To be co-ordinated with the EWI Working Group proposal for a treaty on substantive criminal law.

3. An International Criminal Tribunal for Cyberspace (ICTC)

3.1. An International Criminal Court or Tribunal is needed

Criminal investigation and prosecution based on international law, needs an international criminal court or Tribunal for any proceedings. The International Tribunal shall have the power to prosecute persons responsible for the most serious violations of international cybercrime law, in accordance with the provisions of the present draft Statute of the International Criminal Tribunal for Cyberspace

An international criminal court have been called a missing link in the international legal system. Many most serious global cyberattacks will go unpunished without a criminal court or tribunal in action. When an International Criminal Court or Tribunal is established, then the principle of individual criminal accountability may globally be enforced. Anyone who commits any of the cybercrimes included in the international cybercrime law can be prosecuted by the court. It will be a signal from the United Nations and the global community that global cyberattacks are no longer tolerated.

Cloud computing and multi-jurisdictional crimes may challenge the traditional way of investigation and prosecution, and need an international court or tribunal for the court proceedings.

Data in the "clouds" is data that is constantly being shifted from one server to the next, moving within or access different countries at any time. Also, data in the "clouds" may be mirrored for security and availability reasons, and could therefore be found in multiple locations within a single country or in several countries. Consequently, not even the cloud computing provider may know exactly where the requested data is located.[15]

This problems may only be solved through a global treaty that include jurisdictional provisions for the most serious cybercrimes of global concern.

3.2. Existing International Courts and Tribunals

3.2.1. The International Court of Justice[16]

The Court originates from the early 1900s, based on The Hague Peace Conventions in 1899 and 1907. It became in 1913 the Permanent Court of Arbitration, and moved into the Peace Palace in The Hague, that was built by contributions from Andrew Carnegie.

After the World War 1, the League of Nations established the court as The Permanent Court of International Justice, but it was never a part of the League. The Court did not function after the outbreak of the World War 2, but met for a last time in October 1945.

The International Court of Justice was established by the Charter of the United Nations, which provides that all members of the United Nations are parties to the Courts Statute.

---

[15] INTERPOL European Working Party on Information Technology Crime (EWPITC) – Project on cloud computing, 2011.

[16] See www.icj-cij.org

The Court is the principal judicial organization for the United Nations and started working in 1946.

The International Court of Justice functions as a world court. The Court consists of 15 judges elected for a 9 year period by the United Nations General Assembly and the Security Council sitting independently of each other. No nations may have more than one judge, and elections are held every three years for one third of the judges. A State party to the case may appoint a judge *ad hoc* for the purpose of the case.

The jurisdiction is:
The Court decides, in accordance with international law, disputes of a legal nature that are submitted to the Court by agreement between the States parties to the case. The Court give advisory opinions on legal questions only at the request of the organs of the United Nations and 16 specialized agencies authorized to make such a request. If any doubts occur on the jurisdiction, it is the Court itself which decides.

The judgements are final and without appeal.

3.2.2. The International Criminal Court (ICC)[17]

The Court was established in 1998 by 120 States, at a conference in Rome. The Rome Statute of the International Criminal Court was adopted and it entered into force on July 1st, 2002. The Rome Statute has been ratified or aceeded to by 121 States.[18]

The Court is independent from the United Nations, but has historical, legal and operational ties with the institution. The relationship is governed by the Rome Statute and by other relationship agreements.

The International Criminal Court (ICC) is the first ever permanent, treaty based, fully independent international criminal court established to promote the rule of law and ensure that the gravest international crimes do not go unpunished. The Court do not replace national courts, the jurisdiction is only complementary to the national criminal jurisdictions. It will investigate and prosecute if a State, party to the Rome Statute, is unwilling or unable to prosecute. Anyone, who commits any of the crimes under the Statute, will be liable for prosecution by the Court.

The jurisdiction of the International Criminal Court is limited to States that becomes Parties to the Rome Statute, but then the States are obliged to cooperate fully in the investigation and prosecution. The Court would have no jurisdiction with regard to crimes committed on the territory of non-States Parties, or by their nationals or with regard to States Parties that have declared that they did not accept the Courts jurisdiction over certain spesific crimes.

---

[17] www.icc-cpi.int
[18] Until Juli 1, 2012.

Article 5 limits the jurisdiction to the most serious crimes of concern to the international community as a whole. The article describes the jurisdiction including crimes of genocide, crimes against humanity, war crimes and crimes of aggression.

Individual States may be unwilling or unable to exercise jurisdiction on a case. According to article 17, unwilling is a State whenever it appears to be a lack of genuine will to investigate or prosecute the crime. A State is unable whenever it appears to be a total or substantial collapse of its judicial system, or by some reason is unable to obtain the accused or the necessary evidence and testimony or otherwise unable to carry out its proceedings due to its unavailability.

In the final diplomatic conference in Rome other serious crimes such as terrorism crimes were discussed, but the conference regretted that no generally acceptable definition could be agreed upon. The conference recognized that terrorist acts are serious crimes of concern to the international community, and recommended that a review conference pursuant to the article 123 of the Statute of the International Criminal Court consider such crimes with the view of their inclusion in the list within the jurisdiction of the Court.

The Court was in 2010 seized in five situations. The situations are in Uganda, the Democratic Republic of Congo, the Central African Republic, Darfur in Sudan, and in Kenya. In addition the prosecutor is also conducting preliminary examinations in situations in various other countries around the world.

The International Criminal Court may have a role to play in the fight of massive and coordinated cyberattacks against critical information infrastrutures even today under the current jurisdiction in force. According to article 93, paragraph 10, the Court may upon request " cooperate with and provide assistance to, a State Party conducting an investigation into or trial in respect of conduct which constitutes a crime within the jurisdiction of the Court, or which constitutes a serious crime under the national law of the requesting State."

Massive and coordinated cyber attacks against critical information infrastructures may qualify as a "serious crime".

The Review Conference was held in Kampala on May 31-June 11, 2010. Around 4600 representatives of 84 States (67 States Parties and 17 observers) , intergovernmental and non-governmental organizations attended the Conference. The International Criminal Court was now fully operational as a judicial institution, and the Secretary-General of the United Nations opened the Conference. Some amendments were adopted to the Rome Statute, including a definition of the crime against aggression.

The conference adopted a resolution and decided to retain article 124 in its current form, but agreed to review it again at the 14th session of the Assembly of States Parties in 2015.

The Conference adopted the Kampala Declaration, guided by:

"a firm committment to fight impunity for the most serious crimes of interntional concern and to garantee lasting respect for the enforcement of international criminal justice"

In addition section 12 that reads as follows:

"Decide to henceforth celebrate 17 July, the day of the adoption of the Rome Statute in 1998, as the Day of International Criminal Justice."

A binding global legal instrument such as the Rome Statute of the International Criminal Court may strengthen the global integration of procedural and court proceedings on the most serious crimes of global concern in cyberspace. The Rome Statute may create a global judicial framework ensuring against immunity from the appropriate sanctions of such acts.

If massive and co-ordinated global attacks in cyberspace are included in the jurisdiction of the International Criminal Court, the Rome Statute has Articles on investigation, prosecution and three divisions of Courts for normal and formal proceedings. And the Prosecutor, which is an independent organ of the Court, may after having evaluated the information made available, initiate investigation also on an exceptional basis. (Articles 18 and 53) In accordance with Article 18 on preliminary rulings regarding admissibility, the Prosecutor may *"seek authority from the Pre-Trial Chamber to pursue necessary investigative steps for the purpose of preserving evidence where there is a unique opportunity to obtain important evidence or there is a significant risk that such evidence may not be subsequently available."* Such an exceptional proceeding may very well be needed in investigations of massive and coordinated attacks against critical information infrastructures in cyberspace. It is also the Pre-Trial Chamber that later on eventually issues an arrest warrant.

The Court may exercise its functions and powers on the territory of all States Parties to the Rome Statute, and the maximum term of imprisonment is 30 years, and also a life sentence may be imposed.

3.2.3. The International Criminal Tribunal for the former Yugoslavia (ICTY)[19]

The Tribunal is a United Nations court of law, established in accordance with Chapter VII of the United Nations Charter. The Tribunal was established by the Security Council by passing Resolution 827 on May 25, 1993. The Tribunal's authority is to prosecute crimes committed in the territory of the former Yugoslavia since 1991 and has jurisdiction on issues as follows:

- Grave breaches of the 1949 Geneva Conventions
- Violations of the laws or customs of war
- Genocide
- Crimes against humanity

The Tribunal has concurrent jurisdiction in relation to national courts, but may claim primacy over national courts and take over investigations and proceedings at any stage.

The Chambers consists of 16 permanent judges and a maximum of nine *ad item* judges, all appointed by the United Nations General Assembly. The judges are divided between 3

[19] See www.icty.org

Trial Chambers and one Appeals Chamber. The judges are elected for a period of 4 years. The judges have ensured a fair and open trial, assessing the evidence to determine the guilt or innocence of the accused. The Tribunal has proven that efficient and transparent international justice is possible, and has been setting important precedents of international criminal and humanitarian law.

The Appeal Chamber consists of 7 permanent judges, five from the permanent judges of ICTY and two from the permanent judges of the International Criminal Tribunal for Rwanda (ICTR). These 7 judges also constitute the Appeal Chamber for the ICTR, but each appeal is heard and decided by five judges.

The Tribunal was the first international war crimes tribunal since the Nuremberg and Tokyo tribunals.

The Tribunal has investigated and brought charges against individuals from all ethnic background in the conflicts. The Office of the Prosecutor operates independently of the Security Council, of any State or international organization or other organs of the ICTY. Investigations are initiated by the Prosecutor at his/her own discretion on the basis of information received. Indictments must be confirmed by a judge prior to becoming effective.

The accused are held in the ICTY Detention Unit, located in The Hague. The maximum sentence that may be imposed is life imprisonment. Sentences are served in one of the States that have signed such an agreement with the United Nations.

The judges have also regulatory functions, such as draft and adopt the legal instruments regulating the functions of the Tribunal.

It is estimated that the Tribunal will be functioning into 2013, and the final trial is so far against Karadzic.

3.2.4. The International Criminal Tribunal for Rwanda (ICTR)[20]

The Tribunal was established by the Security Council Resolution 995 on November 8, 1994, in accordance with Chapter VII of the United Nations Charter. It was decided in 1995 that the Tribunal should have its seat in Arusha, Tanzania.

The Tribunal consists of 11 permanent judges appointed in the same manner as the ICTY. The Tribunal has 3 Trial Chambers, and 3 judges serve in each case. The Appeal Chamber consists of 7 permanent judges, five from the permanent judges of ICTY and two from the permanent judges of ICTR. Each appeal is heard and decided by five judges.

The judges have also regulatory functions, such as draft and adopt the legal instruments regulating the functions of the Tribunal.

[20] See www.unictr.org

The jurisdiction on issues is similar to the ICTY.

The jurisdiction otherwise is the prosecution of persons responsible for genocide and other serious violations of international humanitarian law in the period of January 1 and December 1994, committed by Rwandans in the territory of Rwanda, and in the territory of neighbouring States as well as non –Rwandan citizens for crimes committed in Rwanda.

High-ranking individuals, including a former Prime Minister, have been called to account before an international court of law for the first time in history, for massive violation of human rights in Africa with more than 500.000 victims.

3.2.5. The Special Tribunal for Lebanon (STL)[21]

The Government of the Republic of Lebanon requested in December 2005 that the United Nations should establish an International Tribunal for the investigation of the murder of its former prime minister Rafiq Hariri. Persuant to Security Council resolution 1664 (2006) the United Nation and Lebanon negotiated an agreement on the establishment of a Special Tribunal for Lebanon with a majority of international judges and an international prosecutor. Based on the Security Council resolution 1757 (2007), the Statute of the Special Tribunal entered into force in 2007.
The Tribunal is based in Leidschendam-Voorburg, outside The Hague, and began functioning on March 1, 2009. The rules of procedures and evidence is guided by both the Lebanese Code of Criminal Procedure and the rules of prosedures and evidence of other international criminal Tribunals and Courts. The Tribunal does not apply international criminal law, but rather national criminal law of Lebanon. The scope of the Tribunals jurisdiction are: 1) the attack of February 14, 2005, resulting in the death or injury of former Lebanese Prime Minister Rafiq Hariri and others; 2) other attack having occurred between October 1, 2004, and December 12, 2005; and 3) attacks which may have occurred at any later date.
A United Nations International Independent Investigation Commission was established. This Commission is expected to deliver its findings in 2011.
The Tribunal is the first United Nations based international criminal court that tries a "terrorist" crime committed against a specific person.

3.3. An International Criminal Tribunal for Cyberspace (ICTC)

3.3.1. Several seat alternatives

Additional provisions or articles may be included in the list of crimes within the jurisdiction of the International Criminal Court (ICC) in The Hague.

[21] See www.sti-tsl.org

An alternative solution may be to establish a special International Criminal Court for Cyberspace as a subdivision of ICC in The Hague.

The most obvious alternative is a separate International Criminal Tribunal for Cyberspace (ICTC) based on an United Nations Security Council decision. An International Criminal Tribunal for Cyberspace may be seated in The Hague, since it is a natural choice with all international courts inside, or in the urban area of the city.

The INTERPOL Clobal Complex (IGC) will be established and operational in Singapore in 2014, especially on enhancing preparedness to effectively counter cybercrime. Singapore may thus be an alternative seat for an International Criminal Tribunal for Cyberspace. It would open up a possibility of assistance and cooperation with an outstanding investigation institution, that would enable the global justice to promote the rule of law and ensure that the gravest international cybercrimes do not go unpunished.

Investigations and prosecutions of international law need an international criminal court for the independent and efficient proceedings of the most serious cybercrimes of global concern.[22]

The excisting UN based Tribunals have proven that efficient and transparent international justice is possible, and they have been setting important precedents for international criminal law.

3.3.2. A Subdivision of ICC seated in The Hague

An International Criminal Court for Cyberspace may be established as a Subdivision of the International Criminal Court (ICC) and seated in The Hague.

As a Subdivision of the ICC, an International Criminal Court for Cyberspace shall be governed by the Rome Statute. The treaty has provisions on investigation, and prosecution that also will be implemented on a Subdivision. The Prosecutor, as an independent organ of the Court, may after having evaluated the information made available, initiate investigation also on exceptional basis based on a pre-trial decision.

3.3.3. An International Criminal Tribunal for Cyberspace (ICTC)

An International Criminal Tribunal[23] for Cyberspace (ICTC) dealing with the most serious cybercrimes of global concern, could be established in The Hague.

[22] Establishing an international criminal court for cybercrimes has also been unanimously recommended, at a conference on Cyber Security & Law, organized by The Associated Chambers of Commerce and Industry of India (ASSOCHAM) in July 2010. See www.asssocham.org

A Tribunal must be a United Nations court of law, established through a Resolution by the Security Council in accordance with Chapter VII of the United Nations Charter.

The international criminal tribunal will go into action when national criminal justice institutions are unwilling or unable to act on the most serious cybercrimes of global concern. A State may be unwilling to prosecute a cybercrime for any number of reasons, and it may often be lack of will to prosecute their own citizens.

A State is unable to prosecute in cases when its judicial system has collapsed, or when, for some reason, it is unable to capture the accused person or gather the necessary evidence and testimony.

The Chambers

The Chambers should consist of 16 permanent judges and a maximum of nine *ad item* judges, all appointed by the United Nations General Assembly. The judges shall be divided between 3 Trial Chambers and one Appeals Chamber. The judges should be elected for a period of 4 years.

The Appeal Chamber should consist of 7 permanent judges.

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 shall confirm the indictment. If not so satisfied, the indictment shall be dismissed.

The Trial Chambers shall pronounce judgements and impose sentences and penalities on persons convicted of serious violation of international cybercrime law.

Co-operation and judicial assistance

States shall co-operate with the International Criminal Tribunal for Cyberspace in the investigation and prosecution of persons accused of committing serious violations of international cybercrime law.

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 idenfication and locations of persons;

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

(c) the service of documents;

---

23. Tribunals have often been choosen since the formalities are more flexible when established by the United Nations Security Council. The latest Tribunal was decided on at a conference in the Peace Palace in The Hague on October 25, 2010, with the creation of PRIME Finance (Panel of Recognised International Markets Experts in Finance). It will serve as an International Financial Court established in The Hague. See thehagueonline.com

(d) the arrest or detention of persons;

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

Commencement and conduct of trial proceedings

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.

The Rules of Procedure and Evidence must be based on, and in consistent with the Statute of the Tribunal. It should be guided by the Rules of Procedure and Evidence of other international criminal tribunals and courts, such as the ICC, the ICTY and the ICTR.

Enforcement of sentences

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

Imprisonment shall be served in a State designated by the international criminal tribunal from a list of States which 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 criminal tribunal.

Jurisdiction

The jurisdiction of the international criminal tribunal shall be limited to the most serious cybercrimes of corncern 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.

The international criminal tribunal shall exercise jurisdiction over additional cybercrimes according to future decisions of the Statute by the Security Council.

The international criminal tribunal shall have primacy over national courts. At any stage of the prosedure, the tribunal may formally request national courts to defer to the competence of the international criminal tribunal in accordance with the present Statute and Rules of Procedure and Evidence of the Inrenational Criminal Tribunal for Cyberspace.

The international tribunals authority is prosecuting and sentencing cybercrimes, and should have jurisdiction on issues as follows:

- Violations of a global treaty or set of treaties on cybercrime
- Massive and coordinated global cyberattacks against critical communication and information infrastrutures

It is expected that the International Criminal Tribunal for the former Yugoslavia may end its functioning in 2014, leaving both staff and administration building in The Hague available and ready for new tasks.

3.4. The role of Judges in the International Criminal Tribunal for Cyberspace

The three main United Nations international human rights laws of the fundamental individual rights are the Universal Declaration on Human Rights (1948), the International International Covenant on Civil and Political Rights (1966), and the International Bill of Human Rights.

The Universal Declaration of Human Rights Article 19 reads as follows:

> *"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers"*

The role of judges in protecting the rule of international law and human rights in cyberspace should not be different from all other crimes. The United Nations Universal Declaration of Human Rights spell out basic civil, political, economic, social and cultural rights that all human beings should enjoy.[24]

Basic principles for judges is described in the The Magna Carta of Judges (Fundamental Principles), adopted by the Consultative Council of European Judges (CCJE) in 2010.[25]

This Magna Carta of Judges includes the fundamental principles relating to judges and judicial system, and is highly reccommended as global principles adopted in a global Treaty. These fundamental principles contains criteria of the rule of law, the independence of the judiciary, access to justice, and the principles of ethics and responsibility in a national and international context.

The rule of law and justice is described in Article 1 as follows:

> *" 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*"

[24] See www.ohchr.org

[25] Adopted November 18, 2010 by the Consultative Council of European Judges (CCJE). CCJE is a Council of Europe advisory body. See www.coe.int/ccje

A main principle for the judicial independence is described in Articles 2 and 10:

"Judicial independence and impartiality are essential prerequisites for the operation of justice." (Article 2)

"In the exercise of their function to administer justice, judges shall not be subject to any order or instruction, or to any hiearchical pressure, and shall be bound only by law." (Article 10)

These principles shall according to the Magna Carta Article no. 23, apply *mutatis mutandis* to judges of all European and International Courts.

4. The role of Prosecution for the International Criminal Tribunal for Cyberspace

It is The Prosecutors Office that shall be responsible for the investigation and prosecution of persons responsible for the most serious cybercrimes of global consern.

The Prosecutors Office shall act independently of the Security Council, of any State, or any international organization, or of other organs of the Tribunal, as a separate organ of the International Tribunal. The prosecutor shall not seek or receive instructions from any government or from any other source.

Investigations are initiated by the Prosecutor at his/her own discretion on the basis of information received. The Prosecutor may request a judge of the Trial Chamber, to issue such orders and warrants for the arrest, detention, surrender or transfer of persons, and any other orders as may be required for the conduct of the investigation or trial.

Upon 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. Indictments must be confirmed by judges in a pre-trial chamber prior to becoming effective.

The office of the Prosecutor must be managed and headed by a Prosecutor, appointed by the United Nations Security Council by nomination of the Secretary-General. As the Head of the Office he/she should serve a four-year period, and be eligible for reappointment. The office must have the most qualified and experienced staff of prosecutors and investigators that may be required for the investigation and prosecution of global cybercrime. The staff of the Prosecutors Office should be appointed by the United Nations Secretary-General on recommendation by the Prosecutor. The prosecutors and staff should at least serve a two year periode, and also be eligible for reappointment.

The staff of an International Criminal Tribunal for Cyberspace must include experienced and skilled police investigators, prosecutors and other experts on cybercrime from around the world, in A Global Virtual Taskforce. The Prosecutor may then be assisted very efficiently in the determination if a case is of sufficient gravity in order to justify further action by the tribunal.

The Office of the Prosecutor may through INTERPOL be assisted by an international 24-hour response system, including more than 100 countries, that also has been endorced by the High Tech Crime Sub-group of the G8 Group of States. Such assistance may be especially important for the Prosecutors authority to open investigations, on the basis of information about the most serious cybercrimes of global consern within the jurisdiction of the Court, allegedly committed by a national of a State Party or on the territory of a State Party. The Prosecutor may initiate an investigation when there is a reasonable basis to proceed with an investigation.[26]

5. The role of Police investigation for the International Criminal Tribunal for Cyberspace

5.1. Investigation of cybercrime of the most global consern

The Prosecutors Office 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 organisations. The Prosecutor shall assess the information received or obtained and decide whether there is sufficient basis to proceed.

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.

The Prosecutors Office shall have the power to seek assistance in the investigation by INTERPOL and the INTERPOL Global Complex.

[26] See the Rome Statute Article 53.

The Prosecutors Office shall have the power to seek assistance in the investigation also by a Global Virtual Taskforce established by key stakeholders in the global information and communications technology industry, financial service industry, non-governmental organisations, and the global law enforcement.

The Prosecutors Office may be assisted in the global investigation of cybercrimes and cyberattacks of the most global concern, by two pillars:

5.2. INTERPOL

INTERPOL[27] has since the 1980s been the leading international police organization on knowledge about and global cooperation on computer crime and cybercrime investigation, or Information Technology Crime. INTERPOL has since 1990 established Regional Working Parties, or a group of experts, for regional regions in Africa, Asia-South Pacific, The Americas, Europe, the Middle East and North Africa.

These working parties consists of the heads or experienced members of national computer crime units, and have meetings on a regularly basis. The European Working Party has developed the INTERPOL IT Crime Manual.

INTERPOL also organize international conferences on cybercrime every two years for the global law enforcements, and global training courses specializing in Internet investigations.

INTERPOL has established a rapid information exchange system for cybercrimes through the global police communications system I-24/7, where INTERPOL collects, stores, analyses, and shares information on cybercrime with all its member countries. The National Central Reference Points (NCRPs) network for a global cooperation on cybercrime investigation has been endorsed by the G8 High Tech Crime Sub-group, and more than 120 countries are members of the network. This INTERPOL network enables police in one country to immediately identify experts in other countries and obtain assistance in cybercrime investigations and evidence collections. It is very important that the investigators of cybercrimes may swiftly seize digital evidence while most of the evidence is still intact. It is vital that the police have an efficient crossborder cooperation when cyberattacks involves multiple jurisdiction.

The General Assembly of INTERPOL has at their meeting in 2010 approved to establish the INTERPOL Global Complex (IGC), based in Singapore. It is expected to go into full operation in 2014, and to employ a staff of about 300 people.

[27] See information on INTERPOL on www.interpol.int. The headquarter is in Lyon, France.

The IGC is an integral part of the INTERPOLs efforts to reinforce its operational platform and will focus on developing innovative and state-of-the-art policing tools to help law enforcement around the world, especially in enhancing preparedness to effectively counter cybercrime. The IGC will also include a 24-hour Command and Co-ordination Centre (CCC).

Establishing an INTERPOL Global Complex (IGC) in Singapore is a very important effort and development for the international law enforcement to effective counter cybercrime.

5.3. A Global Virtual Taskforce

The Prosecutors Office should have the power to seek the most efficient assistance in the investigation of cybercrimes. A Global Virtual Taskforce established with key stakeholders in the global information and communications technology industry, financial service industry, non-governmental organizations, academia, and the global law enforcement through INTERPOL, working in partnership, will be necessary for the prevention and effectively combat global cybercrimes, especially for delivering real-time responses to cyberattacks. A Taskforce could be overseen by a joint Strategic Working Group.

The Metropolitan Police Central e-crime Unit (PCeU) in partnership with the taskforce in the United Kingdom and the National Cyber Investigative Joint Task Force (NCIJTF) chaired by the FBI in the United States, may be used as a model for a Global Virtual Taskforce.

The International Cybersecurity Protection Alliance (ICSPA) has been established to assist cybercrime law enforcement units around the world. This is a non-government international not-for profit private institution.

A main task for a Global Virtual Taskforce on cybercrime should be to predict, prevent and respond to cybercrime. With regard to cyberattacks, the taskforce should be able to identify, locate and neutralize the attack. A basic platform must also be the coordination and open sharing of knowledge, information and expertise between members of the taskforce, that may result in fast and effective investigative measures and arrests.

6. Draft United Nations Security Council Resolution

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

Noting that the developments of information and communication technologies in cyberspace has resulted in substancial 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 Plenipotentary 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,

Noting the work of international and regional organizations, including the work of the Council of Europe in elaborating the Convention on Cybercrime (2001) and those other organizations in promoting dialogue 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,

7. Draft Statute of The International Criminal Tribunal for Cyberspace (ICTC)

Having been established by the Security Council acting under Chapter VII of the Charter of the United Nations, the International Tribunal for the prosecution of persons responsible for the most serious violations of International Cybercrime Law

(herinafter referred to as "the International Tribunal") shall function in accordance with the provisions of the present Statute.[28]

Article 1

Competence of the International Tribunal

The International Tribunal shall have the power to prosecute persons responsible for the most serious violations of international cybercrime law, in accordance with the provisions of the present Statute.

Article 2

Massive and coordinated global cyberattacks against communications and information infrastructures

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 wilfully 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 defence, public administration and services, public health or safety, or banking and financial services.

[28] The Statute of the International Criminal Tribunal for The Former Yugoslavia has been used as a Model Statute. Articles 13 bis, 13 ter, and 13 quater must be decided at a later stage.

Article 3

Violations of the Global Treaty on Cybercrime[29]

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 wilfully 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

Spam and Identity Theft

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 wilfully against computer systems, information systems, data, information or other property protected under the relevant international criminal law;

a) spam
b) identity theft

Article 5

Preparatory acts of provisions in the Global Treaty on 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,

[29] Article 3-5 to be co-ordinated with the EWI Working Group proposal for a treaty on substantive criminal law.

namely the following acts committed wilfully 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.

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 excecution 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 reponsibility 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 reponsibility, 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 corncern to the international community as a whole. The Tribunal ha 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 prosedure, 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 has already 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 Tibunal 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* independent judges appointed in accordance with article 13 *ter,* paragraph 2, of the Statute, no two of whom may be nationals of the same State.

2. A maximum at any one time of three permanent judges and six *ad item* judges shall be members of each Trial Chamber. EachTrial 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 judgement 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 nine 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 violations of international cybercrime law.

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. 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 organisations. 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 INTERPOL and the INTERPOL Global Complex.

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, financial service industry, non-governmental organisations, and the global law enforcement.

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

5. Upon 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

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 shall confirm the indictment. If not so satisfied, the indictment shall be dismissed.

Article 20

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 21

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 22 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 understands of the nature and cause of the charge against him;

(b) to have adequate time and facilities for the preparation of his defence and to communicate with councel of his own choosing;

(c) to be tried without undue delay;

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

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

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

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

Article 22

Protection of victims and witnesses

The International Tribunal shall provide in its rules of prosedure 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.

Article 23

Judgement

1. The Trial Chambers shall pronounce judgements and impose sentences and penalities on persons convicted of serious violation of international cybercrime law.

2. The judgement 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 24

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 25

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 26

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 revieww of the judgement.

Article 27

Enforcement of sentences

Imprisonment shall be served in a State designated by the International Tribunal from a list of States which 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 28

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 29

Co-operation and judicial assistance

1. States shall co-operate with the International Tribunal in the investigation and prosecution of persons accused of committing serious violations of international cybercrime law.

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 idenfication 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 30

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 staff, and the Registrar and his 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 immunities 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 31

Seat of the International Tribunal

The International Tribunal shall have its seat at The Hague, or at another location according to the Security Council decision.

Article 32

Expences of the International Tribunal

The expences 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 33

Working languages

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

Article 34

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.

Inventory of relevant instruments:

United Nations Office on Drugs and Crime: www.unodc.org

International Telecommunication Union (ITU) www.itu.int

Interpol www.interpol.int/Crime-areas/Cybercrime/Cybercrime

Council of Europe: www.conventions.coe.int

G8 Group of States: www.g7.utoronto.ca

European Union: www.europa.eu

Asia Pacific Economic Cooperation (APEC) http://APEC.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information.aspx

Organization of American States: www.oas.org/juridico/english/cyber_legis.htm

The Commonwealth: www.thecommonwealth.org

Association of South Asian Nations (ASEAN): www.aseansec.org

Organization of Economic Cooperation (OECD): www.oecd.org

The Arab League: www.arableagueonline.org

The African Union: www.africa-union.org

NATO: www.nato.int

Shanghai Cooperation Organization (SCO) www.sectsco.org

References

Gercke, Marco: Understanding Cybercrime – Phenomena, Challenges and Legal Responses, Second edition, (ITU 2011) www.cybercrime.de

Gercke, Marco: National, Regional and International Approaches in the Fight against Cybercrime, (CRi 2008), www.cybercrime.de

Gercke, Marco: The Convention on Cybercrime, MMR (2004)

Gercke, Marco: Internet-related Identity Theft (2007)

Gercke, Marco: Preservation of User Data, DUD (2002)

Goodman, Marc: Crime and Policing in Virtual Worlds (2010) – www.futurecrimes.com

Schjolberg and Hubbard: Harmonizing National Legal Approaches on Cybercrime (2005)

Schjolberg, Stein: Terrorism in Cyberspace – Myth or Reality? (2007) www.cybercrimelaw.net

Schjolberg, Stein: Wanted: A United Nations Cyberspace Treaty - Global Cyber Deterrence (2010) – www.ewi.info

Schjolberg, Stein: A Cyberspace Treaty – A United Nations Convention or Protocol on Cybersecurity and Cybercrime, 12th United Nations Congress on Crime Prevention and Criminal Justice (2010) – www.cybercrimelaw.net

Schjolberg, Stein: Global Supreme Court decisions – www.globalcourts.com

Schjolberg, Stein and Solange Ghernaouti-Helie: A Global Treaty on Cybersecurity and Cybercrime (2011)

Sieber, Ulrich: Council of Europe Organised Crime Report (2004)

Sieber and Brunst: Cyberterrorism and Other Use of the Internet for Terroris Purposes – Threat Analysis and Evaluation of International Conventions (2007)

Sieber, Ulrich: Cybercrime and Jurisdiction in Germany. The Present Situation and the Need for New Solutions, (2006)

Sofaer and Goodman: Cyber Crime and Security - The Transnational Dimension of Cyber Crime and Security (2008)

Viira, Toomas: Meridian, Vol.2 No 1 (January 2008)

Wilson, Clay: Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, CRS Report for US Congress (November 2007)