Potential new global legal mechanisms on combating cybercrime and global cyberattacks

A presentation at the ISPAC International Conference on Cybercrime: Global Phenomenon and its Challenges Courmayeur, Italy

December 2-4, 2011

by
Judge Stein Schjolberg
Norway

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

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, USA

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

[1] Kofi Annan, former UN Secretary-General

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.

Critical information infrastructures of many governments and private industry have been targets by global cyberattacks in the recent year.

The cyberattacks on sensitive national information infrastructure are rapidly emerging as one of the most alarming international security threats, and could be considered as most serious cybercrime of global concern.

Such attacks may have a great potential impact to the global economy, internatioonal security, and the critical information infrastructures of all nations.

2. United Nations

A treaty or a set of treaties at the United Nations level on cybersecurity and cybercrime should be a global proposal based on a potential for consensus. Serious crimes in cyberspace should be established under international law, whether or not they are punishable under the national law of a Party.

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 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.

The United Nations Office on Drugs and Crime (UNODC) in Vienna, Austria organized the 12th of United Nations Congress on Crime Prevention and Criminal Justice in Salvador, Brazil, in April 2010, and the Congress made a recommendation in the Salvador Declaration Article 42. The Commission on Crime Prevention and Criminal Justice and other UN institutions made a follow-up, and the recommendation was adapted by the United Nations General Assembly in its resolution 65/230.

3. Global Working Groups

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

The United Nations has initiated a comprehensive study of the problem of cybercrime, recommended in the Salvador Declaration Article 42 to establish "*an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with the view to examining 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 in January, 2011.[2]

The EastWest Institute (EWI)[3] established in June 2010 a Cybercrime Legal Working Group,[4] in order to advance consideration of a treaty or a set of

[2] See www.unodc.org
[3] See www.ewi.info

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 workshop in Brussels in March, 2011, the second meeting just recently in Lausanne, and the next workshop will be held in March 2012.

United States and the European Union have established a Working Group on Cybersecurity and Cybercrime at the EU-US Summit in November 2010.[5] The group is 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 made additional remarks that large-scale attacks, which is an emerging trend, are not fully covered in the Convention.[6]

4. EWI Cybercrime Legal Working Group Recommendations

The EWI Working Group will make proposals for non-partisan, objective non-political solutions that may promote collaboration and serve as a compromise for the global inter-governmental organizations, and develop a consensus-building set of proposals related to an international criminal law for cyberspace.

Recommendations will include five main pillars:

---

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

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

A. Recommendations for international laws on:

- Substantive criminal law
- Procedural instruments
- Jurisdiction and international cooperation

The recommendations may partly use excisting regional agreements and convention as guidelines or as reference.

B. Establishing A Global Virtual Task Force for the investigation and prosecution

A Global Virtual Task Force should be established, including law enforcements, INTERPOL, non-governmental organizations, key stakeholders in the global ICT industry and sector, financial service industry, academia, working in a partnership.
A task force will be necessary for the prevention, detection, and reponses to the global cybercrimes and global cyberattacks in fast and effective investigative measures and arrests, having real-time access to global information in cyberspace.

C. Establishing an International Criminal Court or Tribunal for Cyberspace (ICTC)

Criminal prosecution based on international law need an international criminal court or tribunal for any proceedings. The most serious cybercrimes of global concern, could be considered in the list of crimes within the jurisdiction of the International Criminal Court (ICC). An alternative solution could be to establish an International Criminal Court or Tribunal for Cyberspace.

D. Recommendations for a global treaty on cybersecurity issues.

Security models for the Information and Communication Technology (ICT) in cyberspace must be developed on a global level, defining a global and national cybersecurity strategy. Technical and procedural measures, organizational structures, capacity building, and international cooperation are the most important issues that should be included in a global treaty.

E. Blocking of child pornography websites

Additional recommendations for a treaty/framework on blocking of child pornography websites will be included. Blocking child pornography websites must be based on global and national solutions.

5. The International Criminal Court (ICC)

The International Criminal Court (ICC)[7] was established at a conference in Rome in 1998 by 120 States. The Rome Statute of the International Criminal Court was adopted and it entered into force on July 1st, 2002.

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.

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*

[7] www.icc-cpi.int

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".

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.

6. An International Criminal Court or Tribunal is necessary

Criminal investigation and prosecution based on international law, needs an international criminal court for any proceedings.

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. This possibility may also be a cornerstone for the global cybercrime deterrence. An effective deterrence may be one of the primary goals for establishing a permanent court or tribunal. It will be a signal

from the United Nations and the global community that global cyberattacks are no longer tolerated.

Provisions may be included in the list of crimes within the jurisdiction of the International Criminal Court (ICC) in The Hague. An alternative solution may be to establish a special International Criminal Court for Cyberspace as a subdivision of ICC in The Hague, since it may be a natural choice with all international courts inside, or in the urban area of this city.

But as an alternative in Singapore, where the INTERPOL Clobal Complex (IGC) will be established and operational in 2013/14 especially on enhancing preparedness to effectively counter cybercrime.

7. International Criminal Tribunal for Cyberspace (ICTC)

An International Criminal Tribunal for Cyberspace 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 Tribunals authority could be prosecuting and sentencing the most serious cybercrimes and global cyberattacks of global concern, 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 information infrastrutures

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

The Office of the Prosecutor should be operating independently of the Security Council, of any State, or any international organization, or of other organs of the Tribunal. Investigations are initiated by the Prosecutor at his/her

own discretion on the basis of information received. Indictments must be confirmed by judges prior to becoming effective.

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 Tribunal for the former Yugoslavia (ICTY) and the Tribunal for Rwanda (ICTR).

An International Criminal Tribunal[8] for Cyberspace could be established in The Hague as the natural choice in 2013-2014.

A possible International Criminal Tribunal for Cybercrime, could as an alternative also be established in Singapore. The tribunal could be operational in time for the opening of Interpol Global Complex (IGC) in Singapore in 2013-14. It would open up a possibility of assistance and cooperation with an outstanding investigation institution.

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 Court. That would enable the global justice to promote the rule of law and ensure that the gravest international cybercrimes do not go unpunished.

[8] 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

8. A global virtual taskforce for the investigation and prosecution of the most serious cybercrimes of global concern

A Global Virtual Taskforce established in operational partnerships 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, will be necessary for the prevention and effectively combat global cybercrimes, especially for delivering fast time responses to cyberattacks.

A basic platform must 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, arrests, convictions, and securing and preserving evidence in a way that ensures legal compliance across many jurisdictions.

The main task for a Global Virtual Taskforce on cybercrime should therefore be to prevent, detect, and respond to cybercrime, by investigation and prosecution of the most serious cybercrimes and cyberattacks of global consern.

A Taskforce could be overseen by a joint global Strategic Working Group.

Establishing an INTERPOL Global Complex (IGC) in Singapore is a very important effort and development for the international law enforcement to effective counter cybercrime. A Global Virtual Taskforce for Cyberspace may also be seated in Singapore. Together, this cooperation may create the most effcient law enforcement support for all global cybercrimes.

The Prosecutor and the office of the Prosecutor shall be responsible for the investigation and prosecution of the most serious cybercrimes of global consern.

The prosecutor must have the ability to act independently in a separate organ of the International Tribunal, and shall not seek or receive instructions from any Government or from any other source.

The Prosecutors Office should have the power to seek the most efficient assistance in the investigation of cybercrimes.

9. INTERPOL

The Prosecutors Office may be assisted in the global investigation by two pillars:

INTERPOL[9] has since the 1980s been the leading international police organization on knowledge about and global cooperation on computer crime and cybercrime investigation.

The INTERPOL network enables police to share information on cybercrime, and 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 INTERPOL Global Complex (IGC) based in Singapore may go into full operation in 2013/14, and employ a staff of about 300 people.

The Global Complex 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.

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

Models for a Virtual Taskforce

The Metropolitan Police Central e-crime Unit (PCeU), was established in UK in 2008. in partnership with the taskforce in the United Kingdom.

The International Cyber Security Protection Alliance (ICSPA) is a business-led global organisation. It is a non-for-profit organisation, established in 2011 to channel funding, expertise and assistance to law enforcement cybercrime units in both domestic and international markets.

The National Cyber Investigative Joint Task Force (NCIJTF) chaired by the FBI in the United States.

DRAFT STATUTE OF THE INTERNATIONAL CRIMINAL TRIBUNAL FOR CYBERSPACE (ICTC)

The United Nations Security Council, acting under Chapter VII of the Charter of the United Nations, has established the International Tribunal for the prosecution of the most serious violations of International Cybercrime Law,

(herinafter referred to as "the International Tribunal") and 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 violations of international cybercrime law, in accordance with the provisions of the present Statute.

Article 2

Violations of 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, 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 3

Violations of other 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, 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 4

Massive and coordinated 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 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.

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, 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 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 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 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.

Conclusion

I would like to conclude my presentation with a statement from Professor Peter Grabosky, Australia:

-Those who fail to anticipate the future are in for a rude shock when it arrives