Peace and Justice in Cyberspace

Potential new international legal mechanisms against global cyberattacks and other global cybercrime

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

By Judge Stein Schjolberg, Court of Appeal,
Norway
(2012)

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
(2010)

Potential new international legal mechanisms against global cyberattacks and other global cybercrime

"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. An International Criminal Court or Tribunal for Cyberspace

The most serious global cyberattacks in the recent years, have revealed that almost nobody has been investigated, and nobody has been prosecuted and sentenced. 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.

The international community reached on July 17, 1998, an historic milestone in the development of a permanent International Criminal Law, when 120 States adopted the Rome Statute of the International Criminal Court. 160 States was present in Rome and it is understood that launching the Rome Statute was based on complete consensus among all present States.
The Rome Statute entered into force on July 1, 2002, after ratification of 60 States. At the 10th Anniversary on July 1, 2012, 121 States have made their ratification. China, Russia, and the United States have not made a ratification of the Rome Statute of the International Criminal Court.

An independent Criminal Court or Tribunal for Cyberspace is urgently needed to enable the global justice to take measures on global cyberattacks of the most serious global concern against critical government and private industry information infrastructures or endanger peace.

These could be ensured by expanding the jurisdiction of the International Criminal Court. Considering the ratification positions, any Court solution for Cyberspace that may include acceptance by China, Russia, and the United States.

A Tribunal, that traditionally is a preliminary solution, is currently the only global alternative. After some years of experience, the global community may then try for a more permanent global court solution for cyberspace.

2. The structure of an International Criminal Tribunal

The United Nations Security Council should under Chapter Seven of the United Nations Charter establish an International Criminal Tribunal for Cyberspace for the investigation, prosecution, and sentencing of global cyberattacks. The United Nations Charter is a constituent treaty, and it is binding for all members of the United Nations.

The United Nations Security Council have previously asserted its rights, authority and jurisdiction based on the United Nations Charter, when it established the International Criminal Tribunal for Rwanda and the International Criminal Tribunal for the former Yugoslavia.
The United Nations Security Council has always authority to refer cases to the International Criminal Tribunal for Cyberspace, and may request for an investigation.

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 and acts of cyber warfare.

Peace and justice in cyberspace should be protected by international law through a treaty or a set of treaties under the United Nations.

An International Criminal Tribunal for Cyberspace should be a fully independent international criminal tribunal established to promote the rule of international law and ensure that the gravest global cyberattacks in cyberspace do not go unpunished.

The Chambers of an International Criminal Tribunal for Cyberspace should consist of 16 permanent judges, all appointed by the United Nations. The judges could be divided between 3 Trial Chambers and one Appeals Chamber. The judges should be elected for a period of at least 4 years.

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

The Seat of the International Criminal Tribunal could be The Hague, or Singapore, or both.

3. Prosecution for the International Criminal Tribunal

The Prosecutor, as a separate organ of the International Criminal Tribunal for Cyberspace, should be responsible for the investigation and prosecution of the most serious cyberattacks or 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 Criminal Tribunal.

The Prosecutor should not seek or receive instructions from any government or from any external source. The prosecutor could be advised by the Prosecutors Advisory Board that may consists of five prosecutors appointed from the five veto-wielding permanent members of the United Nations Security Council – China, France, Russia, United Kingdom, and United States.

One alternative may be that the Advisory Board five members could have the power of each to veto any indictments before the International Criminal Tribunal for Cyberspace. Abstenation is not regarded as a veto.

Prosedural matters should not be subject to a veto, and a veto should not be used to avoid a decision by the Prosecutor of opening of any investigation, or to avoid discussions of an issue.

4. Investigation for the International Criminal Tribunal

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

a. Global law enforcements through the coordination of INTERPOL, and

b. A Global Virtual Task Force.

a. The General Assembly of INTERPOL has at their meeting in 2010 approved to establish the INTERPOL Global Complex for Innovation (IGCI), more recently including a Digital Crime Centre, based in Singapore. It is expected to go into full operation in 2014, and to employ a staff of about 300 people.

The INTERPOL Digital Crime Centre (IDCC) will be grouped in three main areas: cybercrime investigative support, research and innovation, and cybersecurity. The IDCC is expected to:

"to serve as a global hub for cybercrime issues, coordinating with national cybercrime investigatigators and authorities in INTERPOL´s member countries and with private partners in the technology industry. The IDCC will bring all affected groups together to generate innovative solutions leading to the ultimate goal of creating a secure cyber world."

b. The Prosecutors Office should have the power to seek the most efficient assistance from experts in a Global Virtual Taskforce, established with key stakeholders in the global information and communications technology industry, financial service industry, private sector, non-governmental organizations, academia, and the global law enforcement through

INTERPOL. That may include experts from Google, Facebook, YouTube, Apple, Microsoft, and more.

A Global Virtual Taskforce for the investigation and prosecution of global cyberattacks and other cybercrimes should be working together in a strong partnership, to coordinate, integrate and share information for the prevention and effectively combating such global crimes, especially for delivering real-time responses to cyberattacks. The goal is to ensure that all global legal means and resources available are used to prevent, identfy, and take real-time actions against cyber threats of the most global concern.

The experts in an international taskforce should be working together as fully integrated task force partners in daily operations, either at the International Criminal Tribunal or in a Virtual collaboration.

The Partnership could be agreed on in Memorandum of Understanding (MoU) with each of the partners.

Such partnership may dramatically improve the Prosecutors Office ability to investigate and prosecute global cyberattacks.

5. Substantive criminal law in the Statute for an International Criminal Tribunal

No international substantive cybercrime law has been recognized globally.

Several governments, international organizations, and vital private institutions in the global information and financial infrastructures have been targets by global cyberattacks in the recent years.

Cyberattacks of the most serious global concern, that intentionally causes substantial and comprehensive disturbance against critical communications and information infrastructure, should be included in a Statute for a International Criminal Tribunal.

Illegal access, illegal interception, data interference, system interference, misuse of devices, forgery, fraud, and offences related to child pornography, could also be included in the Statute. Those acts may be prosecuted independently, whenever the conducts are considered as of the most serious cybercrimes of global concern. But the most practical applications may be as included in indictments on global cyberattacks.

Including infringements on religious or political values in cybercrime legislation should be avoided.

A proposal for a provision on global cyberattaks against critical communication and information infrastructure, may be as follows:

"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 communication 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."

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

Professor Peter Grabosky

Australia