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

A presentation at the
International Criminal Law Network (ICLN) Annual Conference
The Hague, the Netherlands
December 13, 2012

By
Judge Stein Schjolberg, Court of Appeal,
Norway

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-)

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

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, a 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 were 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 necessary 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 must be limited to a Tribunal.

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.

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.

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 treaty, and it is binding for all members of the United Nations.

Peace and justice in cyberspace should be protected by international law through a treaty or a set of treaties under 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.
These Tribunals have proven that efficient and transparent international justice have been possible, in addition to setting important precedents for international criminal law.

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 jurisdiction of a Tribunal should be limited to the most serious cybercrimes of global concern.

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 Rules of Procedure and Evidence should be based on, and in consistent with the Statute of the Tribunal. It should be guided by the Statutes of the International Criminal Court and the other Tribunals.

The Seat of an International Criminal Tribunal should be where it is considered necessary for an efficient exercise of its funtions. It 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 Global Complex, including the Digital Crime Centre will be established and operational in Singapore in 2014. Singapore may then be an alternative seat for a Tribunal.
The Seat of an International Criminal Tribunal could be The Hague, or Singapore, or both.

3. International Working Groups

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, in order 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. This study group is organized by the UNODC in Vienna, *"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 2011.[1]

A questionnaire was in February 2012 sent to all United Nations Member States, the private sector, IGOs and academia, and regional workshops were organized.

The drafting and finalization of the study will be carried out before March 2013, with a view of presentation the report to the United Nations Crime Commission in April 2013.

The EastWest Institute (EWI)[2] has in June 2010, established a Cybercrime Legal Working Group,[3] 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 in March 2011.

Proposals for global recommendations was presented at the 3rd EWI Worldwide Cybersecurity Summit in October 2012 in New Dehli.

The final recommendations will be presented at the next Cybersecurity Summit in Silicon Valley in November 2013.

United States and the European Union have established a Working Group on Cybersecurity and Cybercrime at the EU-US Summit in November 2010.[4] The group is

[1] See www.unodc.org

[2] See www.ewi.info

[3] 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.

[4] 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.[5]

The Working Group organized in November 2011 the Cyber Atlantic 2011 exercise.[6]

The Commonwealth has at the Meeting for Law Ministers and Attorney-Generals from 44 countries in Sydney, July 2011,[7] recommended that the Commonwealth Secretariat established a Working Group of experts. The mandate to this Working Group by the Commonwealth Law Ministers is to identify inter alia the most effective means of international cooperation and enforcement, with respect to investigating and prosecuting cybercrime.

The next meeting is in March, and they hope to present report to the Commonwealth Secretariat by June 2013.

4. 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 Prosecutor should not seek or receive instructions from any government or from any external source. The prosecutor could be advised by a 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.

---

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

[6] See http://enisa.europa.eu

[7] See www.thecommonwealth.org

5. Investigation for the International Criminal Tribunal

The Prosecutors Office should be assisted in the investigation of cyberattacks of 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.

The current law enforcements requests across national borders may often today be very slow and complicated. Especially for requests including social networks in Cyberspace.

In the worlds most serious murder case in 2011, where 68 young people was brutally murdered one by one, in addition to the destruction of three Governments buildings and death of additional 9 people, the responses from Facebook were not available before the Court Trial opened in Oslo in April 2012. The requests were sent several months before.

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 in virtual ”meeting rooms”.

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.

6. 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 the main provision included in a Statute for an 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."

I would like to conclude my presentation with another statement:

"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)