Crossing jurisdictional boundaries

by

Judge Stein Schjolberg, (Ret.)
Norway

A presentation at the Europol-INTERPOL Cybercrime Conference

September 24-25, 2013
Europol Headquarter
The Hague, The Netherlands

Chairman, High Level Experts Group (HLEG), ITU, Geneva, (2007-2008)
Chair, EastWest Institute (EWI) Cybercrime Legal Working Group, (2010-2013)

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

I. The Background

Together with INTERPOL I organized The First Interpol Training Seminar for Investigators of Computer Crime in 1981.[1] We were 66 investigators and prosecutors from 26 countries that participated.

In the summary from this first step on the development of legal mechanisms on combating computer crime around the world, I concluded as follows:

"If more than one country is involved, it emphasize the need to harmonize penal codes through guidelines or recommendations to assure proper prosecution, which otherwise could be prevented by international jurisdictional problems."[2]

OECD in Paris was the first organization that followed up and developed Recommendations, but The Council of Europe became the main organization in developing Recommendations and a Convention on Cybercrime.

International and regional organizations have today developed binding cybercrime instruments:

- The Council of Europe Convention on Cybercrime in 2001
- The League of Arab States Convention on Combating Information Technology Offences,
- The Commonwealth of Independent States Agreement on Cooperation in Combating Offences related to Computer Information,
- The Shanghai Cooperation Organization Agreement in the Field of International Information Security

Globally at least 82 countries have signed and/or ratified a binding cybercrime instruments. But it have today resulted in fragmentation at the international level, and a diversity of national cybercrime laws.

II. The Challenges

The framework of challenges for the future lies in a principle decribed by Kapil Sipal, the Minister for Communication and Information Technology in India, at a cybersecurity summit in India in 2012 as follows:

"It is no longer a question of a nation protecting its own security, it is a question of the global community protecting itself."

---

[1] The Conference was organized by Interpol in co-operation with Stein Schjolberg, It was attended by 66 delegates from 26 countries. The keynote speaker at the Conference was Donn B. Parker, SRI International, Menlo Park, California, USA, the "founder" of the combat against computer crime.

[2] Stein Schjolberg: EDP and Penal Legislation, A presentation at the Interpol Conference in December 1981. In cooperation with SRI International, USA, The Norwegian Research Center for Computers and Law, University of Oslo, and Interpol, Paris, he was working on a model law for computer crime laws that could be used as a remedy, or guideline for other countries.

1.Traditional investigation principles are old-fashioned

Traditional investigation principles and methods are old-fashioned and will not be sufficient in obtaining volatile electronic evidences. To gather crossborder electronic evidence is very time-consuming. Law enforcements are still using legal principles from the 1990ties in crimes on social networks, which today have an increasing important role and is a part of any criminal investigation.

New means of formal international cooperation in crossborder investigation must be established.

2. Global cyberattacks against communications and information infrastructures

Several governments, international organizations, and vital private institutions in the global information and financial infrastructures have been targets on a daily basis by global cyberattacks in the recent years.
The development of the most serious cyberattacks on critical government and private industry information infrastructure, have revealed a necessity for implementing a separate provision on the most serious cyberattacks of global concern, without being considered as cyber warfare, in a statute for new legal mechanisms in cyberspace.

Global cyber attacks against critical communication and information infrastructures should be included in a treaty for a global Statute since it have not yet been regulated by international law.

3. The social networks

A social networking service is a platform to build social networks or social relations among people who, share interests, activities, backgrounds, or real-life connections.

Most offences in the sosial networks may be covered by the traditional criminal laws, but very often not sufficiently.

The development of unacceptable behaviour on social networks must be followed very closely. If special legal interests needs protection by criminal law, special legal measures may be necessary. Such interests would be global, and may also be included in future global treaties.

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 Norway in addition to the destruction of three Governments buildings and death of additional 9 people, all the responses from Facebook were not available before the Court Trial opened in Oslo in April 2012. The requests were sent several months before.

4. Cloud computing

Cloud computing and multi-jurisdictional crimes may challenge the traditional way of investigation and prosecution

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.[3]

III. International Working Groups

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

1. United Nations

The United Nations 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."

Information was received from 69 member States and from 67 non-governmental organizations.

The last Meeting was held in Vienna, February, 2013. The Meeting agreed on recommendations for technical assistance and capacity building. Proposals for new national and international legal responses to cybercrime did not reach any possibility for a consensus.
In the current situation there is a "deadlock" on issues of international treaties for legal measures.

The Study Report emphasized that in the future hyper-connected global society, any crime may involve electronic evidence linked with the Internet connections, and:

"require fundamental changes in law enforcement approach, evidence gathering, and mechanisms of international cooperation in criminal matters."

---

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

2. EastWest Institute (EWI)

The EastWest Institute (EWI) established in June 2010, a Cybercrime Legal Working Group, 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.
I am the Chair of this Working Group.

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 final recommendations will be presented to the World Cyberspace Cooperation Summit in Silicon Valley in November 2013.

The Working Group has presented proposals for a draft United Nations Statute on an International Criminal Court or Tribunal for Cyberspace, and a draft United Nations Treaty on combating online child sexual abuse

3. United States and European Union

United States and the European Union have also established a Working Group on Cybersecurity and Cybercrime at the EU-US Summit in November 2010.

Russia has declared that it will never sign or ratify the Council of Europe Convention on Cybercrime, and together with China and a number of other countries suggests the preparation of a new agreement to combat cybercrime.
Russia has in January 2013 made the following statement:

" During this 10 years, cyberspace has changed so greatly that Russia, China and a number of other countries insist on the preparation of a new agreement to combat cybercrime."

4. The Commonweath

The Commonwealth established a Working Group in 2011.

The Working Group Report was finalized at a meeting in May 2013, and it was submitted to the Senior Officials in September, to be presented to the Commonwealth Law Ministers in 2014.

5. ITU

The International Telecommunications Union (ITU) has at a World Conference on International Telecommunication meeting in Dubai in December 2012 initiated changes to the International Telecommunication Regulations (ITR), a global treaty from 1988. At the Meeting 89 States voted for giving ITU the jurisdiction over the operations and content of the Internet, and 55 States voted against.

The next stage of the decision making will be the ITU Conference in Busan, South Korea in October 2014.

Some States prefer to establish an international control over the Internet, and restrict Internet access within their own borders. It is estimated that more than 40 countries (December 2012) filters Internet for what their citizens shall see. These countries often orders websites to censor themselves for political and religious content, in addition to block access to global social media such as Facebook, YouTube and Twitter.

6. UNODC Key Findings

Two of the key findings from the UNODC Study Group, shall be mentioned:

1. Reliance on traditional means of formal international cooperation in cybercrime matters is not currently able to offer timely response needed for obtaining volatile electronic evidence. As an increasing number of crimes involve geo-distributed electronic evidence, this will become an issue not only for cybercrime, but all crimes in general.
2. In a world of cloud computing and data centres, the role of evidence ”location” needs to be reconceptualized, including with a view to obtaining consensus on issues concerning direct access to extraterritorial data by law enforcement authorities.

IV. The Solutions for the investigations

1. Police investigation

INTERPOL has since the 1980s been the leading international police organization on global cooperation of computer crime and cybercrime investigation. The global law enforcements should continue to be coordinated by INTERPOL, as the leading global law enforcement, also in the coordination and investigation of criminal offences in cyberspace.

Regional police organization such as Europol may be excellent partners for collaboration and partnership.

2. A Global Virtual Task Force for Cyberspace

A Global Virtual Taskforce for Cyberspace should be 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 coordinated by INTERPOL. A Global Virtual Taskforce may then hopefully include the assistance from global companies such as Google, Facebook, YouTube, Apple, Microsoft, and many more.

A Global Virtual Taskforce for the investigation and prosecution of global cyberattacks and other cybercrime should be working together in a strong partnership based on Memorandum of Understanding (MoU) to coordinate, integrate and share

information for the prevention, and effectively combating such global cybercrimes, especially for delivering real-time responses to cybercrimes.

A Taskforce working together in virtual "meeting rooms" or virtual environments, will be vital in identify and address global cyber criminals across jurisdictional boundaries.

V. Judicial cooperation

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

Benjamin B. Ferencz,
Former US Prosecutor

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.

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.

An international criminal court have been called a missing link in the international legal system.

In the current lack of judicial cooperation among global countries, 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.

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

This could be ensured by expanding the jurisdiction of the International Criminal Court. But considering the ratification positions for the International Criminal Court, any solution that may include acceptance by China, Russia, and the United States must today 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.

It will be of great importance for peace, justice an security in cyberspace today, and a signal from the United Nations and the global community that global cyberattacks are not tolerated. The establiment of an International Criminal Tribunal for Cyberspace,

and the prosecution of perpetrators will also contribute to the deterrence of global cyberattacks.

VI. Is a new mechanisms for judicial cooperation such as an International Court or Tribunal for Cyberspace really needed?

If we read the responses from 69 countries in the UNODC Report[4] to the questionnaires, it should not be any need.

The countries report that between 30 and 70 % of cybercrimes involve a transnational dimension. Such dimension arises ”where an element or substantial effect of the offence is in another territory, or where part of the modus operandi of the offence is in another territory”.

The responses reveales that a region such as Europe consider the national laws to be sufficient frameworks for prosecuting extraterritorial cybercrimes. But in other regions almost 50% of the countries reports of insufficient legal frameworks. In many countries jurisdictional conflicts may be resolved through formal and informal consultations between countries.

The UNODC points out that if one read the country responses, they do not reveal any need for additional forms of jurisdiction over a putative cyberspace dimension.

But UNODC found that it could not be the correct global conclusion.

UNODC pointed out that the use of traditional forms of judicial cooperation basicly was obtaining extra-territorial evidence in cybercrime cases, with 70 % using formal mutual legal assistance requests for this purpose. In almost 60 % of these cases requests used bilateral instruments as the legal basis. Multilateral instruments were only used in 20 % of the cases. For both categories, the response time were in months. UNODC noted that this may ”present challenges to the collection of volatile electronic evidence.”

Using the 24/7 networks represents important potential for a faster response time, but handles only 3 % of cybercrime cases of the reporting countries.

---

[4] Expert Group to Conduct a Comprehensive Study on Cybercrime – Executive Summary, January 23, 2013 (UNODC/CCPCJ/EG.4/2013/2) see www.unodc.org

The formal requirement of the State consent, whenever the sovereignty of individual State is affected by foreign law enforcement investigations, are increasingly no longer a rule that are followed.

Direct access to data by investigators may often occur without any consent from the country where the data centre is physically located.

Existing regional instruments are focusing on the consent from the person having lawful authorithy to disclose the data, and will therefore not cover such investigative situations adequately.

Cloud computing and multi-jurisdictional crimes may challenge the traditional way of investigation and prosecution, and need a new international legal mechanisms.

UNODC also emphasize the risks of the emergence of clusters of countries with necessary procedures to cooperate among themselves in investigations, but require traditional formal requests for all other countries. The lack of common approach, may result in difficulties for those countries to have their requests for actions fulfilled.

UNODC concludes as follows:

”Globally, divergences in the scope of cooperation provisions in multilateral and bilateral instruments, a lack of response time obligation, a lack of agreement on permissible direct access to extraterritorial data, multiple informal law enforcement networks, and a variance in cooperation safeguards, **represent significant challenges to effective international cooperation regarding electronic evidence in criminal matters.**”

In my opinion, it means that the country responses that may not reveal any need for additional forms of jurisdiction over a putative cyberspace dimension, is insufficient.

New global legal mechanisms are needed in preventing and combating global cyberattacks, and promote an effective international cooperation on the United Nations level.

VII. The Prosecutor at an International Tribunal

If the establiment of an International Criminal Tribunal for Cyberspace is needed, it is the Prosecutor as a separate organ of the Tribunal, that should be responsible for the investigation and prosecution of anybody responsible for the most serious cyberattacks and other cybercrimes of global concern.

The Prosecutors Office should act independently of the Security Council, of any State, or any international organization, or of other organs of the Tribunal.

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

The Prosecutors Office should 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 and cooperation from the prosecutors or judicial authorities in all countries involved.

The Prosecutors Office may have cooperation in the global investigation of cyberattacks and other cybercrimes of the most serious global concern, by two pillars:

- Global law enforcements coordinated through INTERPOL,
- A Global Virtual Taskforce for Cyberspace, including key stakeholders in the global private sector and the global law enforcement coordinated by INTERPOL

The Prosecutor should not seek or receive instructions from any government or from any external source. The prosecutor could, as an alternative, 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, the United Kingdom, and the United States.
The Advisory Board five members could have each the power 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, so the veto can not be used to avoid the decision of opening of any investigation by the Prosecutor or to avoid discussions of an issue. The same includes certain procedural decisions by the Prosecutor that directly regards permanent members.

A ”Mock Trial” could be planned in conjunction with the discussions, as an example on how an International Criminal Court or Tribunal for Cyberspace could be functioning.
The demonstration trial should be based on the assumption of a future UN based treaty or a set of treaties on an international criminal tribunal for cyberspace, a global virtual task force for Cyberspace for the investigation and prosecution, and an international criminal law on global cyberattacks and other cybercrimes of the most serious global concern.

VIII. The International Criminal Court (ICC)

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. Currently (October 2013) 122 States have ratified the Treaty. China, Russia, and the United States have not made a ratification of the Rome Statute.

IX. An International Criminal Tribunal for Cyberspace

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 of the most global concern. The United Nations Charter is a constituent treaty, and a Security Council decision is binding for all members of the United Nations.

The most obvious alternative is a separate International Criminal Tribunal for Cyberspace based on an United Nations Security Council decision.

The International Criminal Tribunal for Cyberspace should be a treaty based, fully independent international criminal tribunal established to promote the rule of law and ensure that the gravest international crimes in cyberspace do not go unpunished.

The jurisdiction of the International Criminal Tribunal for Cyberspace is limited to States that becomes Parties to the Statute, but then the States are obliged to cooperate fully in the investigation and prosecution.

All judges should have experiences as judges, or other similar background in criminal law and international law.

The Tribunal should decide, in accordance with international criminal law, cases that are submitted to the Tribunal by the Prosecutor.
The Tribunal may give advisory opinions on international cybercrime legal questions.

1. Several seat alternatives

An International Criminal Tribunal for Cyberspace may be seated in The Hague, since it is a natural choice with all its international courts, or in the urban area of the city. But the Tribunal should sit elsewhere when it considers it necessary for the efficient exercise of its functions.

The INTERPOL Global Complex for Innovation, including the Digital Crime Centre will be established and operational in Singapore in 2014, especially for enhancing preparedness to effectively counter cybercrime. Singapore may thus be an alternative seat for an International Criminal Tribunal for Cyberspace.

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

2. The Chambers

The judges should be divided between 3 Trial Chambers and one Appeals Chamber.
The judges should be elected for a period of 4 years.
Five of the judges should be appointed from each of the five veto-wielding permanent members of the United Nations Security Council – China, France, Russia, the United Kingdom, and the United States.

3. Jurisdiction

The jurisdiction of the international criminal tribunal should be limited to the most serious cybercrimes of concern to the international community as a whole. The tribunal should have jurisdiction in accordance with the Statute with respect to the included criminal provisions.

The international criminal tribunal should have primacy over national courts. At any stage of the procedure, the tribunal should formally request national courts to defer to the competence of the international criminal tribunal, in accordance with the present Statute and provisions on rules of procedure and evidence.
If any doubts occur on the jurisdiction, it is the Tribunal itself that decides.

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

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.

Basic principles for judges is described in the The Magna Carta of Judges (Fundamental Principles), adopted by the Consultative Council of European Judges in 2010.[5]
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 as follows:

[5] 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

" 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" (Article 1).

A main principle for the judicial independence is described:

"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 should according to the Magna Carta Article no. 23, apply to judges of all European and International Courts.

Thank you very much for your attention.