Ideas on the Establishment

of an

International Court for Cyber Crime

The Best Way to Shape the Future is to Understand the Present

Prof. W. Kraft PhD

in cooperation with

Dr. Claudia Streit

Preamble

The World Council for Law Firms and Justice promotes the evaluation and harmonisation of the legal systems throughout the world. There are many small and many great steps on the road to fulfilling this vision. This consideration of ideas on the establishment of an International Court for Cybercrime is intended as the start of an international initiative to mark an important milestone on the long road.

The idea grew out of the development of a programme for an international WCLF conference on internet criminality, planned to take place next year in Hamburg. International criminal investigation and punishment of crimes in cyberspace naturally came up on the agenda. Obviously, the existing legal resources are nowhere near adequate to keep up with the unbelievably rapid development of the Internet and the associated international criminal ingenuity. The establishment of an international criminal court for the prosecution of Internet crimes could wholly or partially reduce the criminals' lead. The realisation of this vision requires expertise, commitment and courage – including the courage to ignore borders and dogmas and to think consistently towards the future.

The following comments are merely early signposts on the road, opening with a look at existing initiatives showing how virulent the subject is, but also how far the ideas about an international agreement differ. Efforts to date to harmonise legal systems will then be followed by an outline of the tasks which could be undertaken by a WCLF working group on an International Court for Cybercrime which could establish important links to other organisations and would then be in a position to set a visible mark for justice throughout the world.

As far as the future is concerned
it is not your task to envision it,
but rather to make it possible.

Antoine de Saint-Exupéry

© WCLF 2011

1. What is covered by the term "Cybercrime"?

The terms "Cybercrime" and "Internet criminality" are not exactly coextensive - Cybercrime covers both the German concept of computer criminality and Internet criminality. They will be used below in that sense. Cybercrime therefore covers crimes

- in which a computer or a computer network is the target of the attack.
- in which a computer or computer network is the ***instrument*** of the attack.[1]

The first category includes unauthorised access to computers or computer networks, the theft of data, "salami attacks", Trojans and "logic bombs". In the second category are, for example, financial crimes, the sale of illegal articles, child pornography, illegal Internet betting and Intellectual Property offences.

Parallel to the classification according to the method of commission of the crime, another sub-classification can be made according to victims. Cybercrimes can be committed against

- ***individuals*** (with further distinction according to persons and personal property)
- ***organisations,*** or
- ***society as a whole.***

Crimes against organisations could be, e.g. unauthorised access to or control over a computer system, unauthorised acquisition and possession of information and cyber terrorism against governmental organisations. The spread of child pornography, illegal trafficking of persons or drugs and financial crimes are directed against society as a whole.[2]

2. Lack of uniformity between national legislation

There is no global agreement in detail on what acts in cyberspace should be described as criminal. While most countries and regional organisations have, in the past 20 years, introduced legislation and a legal framework within which to combat cybercrime and although similarities can be discerned, the legislative differences remain significant. There are many reasons why this is so. Firstly, the same act can have effects of significantly differing intensity in different states. Secondly, legal comprehension differs; what is illegal in one state is regarded in another as the self-evident exercise of freedom.

A degree of approximation in legal understanding and of legislative harmonisation is necessary if international investigations and prosecution were to function.[3] Many existing legal assistance treaties are based on the principle of "dual criminality": Only if an act is illegal in both countries, will legal assistance be rendered. And, of course, international legislation in the form of an international convention and international jurisprudence of an international court is at all only possible only with fundamental agreement between states.[4]

---

1 After M. Ayilyath, Cyber Crimes and the Legal Framework against it – International and Indian Perspectives, October 2010, p. 1 [= Ayilyath 2010]. The third category – crimes in which a computer(network) is only incidentally involved – is ignored here because it is not relevant for an International Criminal Court.

2 Ayilyath 2010, p. 2

3 Draft Topics of the Vienna meeting of the UN Expert Group on Cybercrime of 17.-21.01.2011, UNODC/CCPCJ/EG.4/2011/2, [= UNODC Expert Group 2011], p. 8/9

4 The problem, included in the Lisbon Treaty as an objective, of the introduction of a European public prosecutor is similar. No progress has been made because a uniform criminal law basis is missing even within the EU. cf. e.g. Silke Nürnberger, Die zukünftige Europäische Staatsanwaltschaft – eine Einführung, in: ZJS 5/2009, p. 494-505

3. International Criminal Prosecution at present

In principle, there are four sources for a legal basis for international criminal prosecution cooperation: extradition, mutual legal assistance and cooperation on seizures can take place firstly, on the basis of international or regional conventions on the prosecution of certain crimes - the European Convention on Cybercrime falls into this category - secondly, on the basis of regional treaties on international cooperation on combating crime in general, e.g. already existing extradition and legal assistance treaties. Bilateral treaties on the same issues and national law may, finally, permit international cooperation case by case.[5]

Finally, conventions on the mutual recognition of national judgements can also be relevant. “The Hague Convention on Foreign Judgments in Civil and Commercial Matters“ of 1971 and the “EC Convention on Jurisdiction and the Enforcement of Judgment in Civil and Commercial Matters“ of 2000 are examples.[6] In view of the limited number of signatories to the latter Convention[7], it can already be imagined how difficult states find it to surrender the sovereignty of their court judgements.

The existing possibilities of legal assistance and international cooperation in combating cybercrime are overwhelmingly regarded as being inadequate.[8]

4. Existing international legal environment

It seems to be generally accepted that the Council of Europe Convention on Cybercrime– together with the Commonwealth Model Law on Cybercrime – has developed the most comprehensive approach to an international legal framework since it covers both criminal law and procedural law as well as questions of international legal cooperation.[9]

The Convention defines a large number of cybercrimes, including illegal access, illegal interception, data and system interference, computer-related forgery and fraud, offences related to child pornography and offences related to infringement of copyright.[10] Listing the details of the Convention here would be outside the bounds of this article. In connection with the idea of an International Criminal Court for Cybercrime, however, it is interesting that the signatories undertake to introduce the legal mechanisms and procedures necessary for the prosecution of cybercrimes.
In addition, the signatories undertake to introduce legislation on data recording so that data is available in the event of a criminal investigation. A signatory must also authorise one of its institutions to access computer systems under defined conditions for the purposes of investigation.[11] Finally, Chapter III states that the parties to the Convention shall cooperate to the widest extent possible for the purposes of investigating criminal offences on the basis of uniform or reciprocal legislation. [12]

---

5 UNODC Expert Group 2011, p. 12
6 Ayilyath 2010, p. 8
7 Die EC Convention was signed only by the Czech Republic, Estonia, Cyprus, Latvia, Lithuania, Hungary, Malta, Poland and Slovenia and the Slovak Republic.
8 This position is shared by German Internet criminal law experts within the WCLF. cf. e.g. Dr. Jürgen-P. Graf, Aktuelle Rechtsprechung des BHG zu Fragen der Internetkriminalität, Vortrag bei der Deutschen Richterakademie, 27.3.2010, p. 64
9 UNODC Expert Group 2011, p. 16, with many others.
10 Ayilyath 2010, p. 7
11 Ayilyath 2010, p. 6
12 Ayilyath 2010, p. 7

5. Working Groups on the creation of effective instruments for legal enforcement at the international level

- **UN Commission on Crime Prevention and Criminal Justice (UNODC) - *Intergovernmental expert group on Internet crime***

  The intergovernmental expert group on Internet crime of the UNODC was established in 2010 with the task of considering possibilities of effectively proceeding against Internet crime. It is required to consider how existing judicial mechanisms can be strengthened and/or to propose new national and international judicial or other measures against Internet crime. The agenda of the first (and so far, only) meeting of the group [13] considered the following legal areas: harmonisation of legislation, substantive criminal law, investigation instruments, international cooperation in law enforcement, securing of electronic evidence, liability of Internet service providers. But non-judicial measures and strategies were also considered, including technical investigation possibilities and defence strategies of the private sector against Internet criminality. The first meeting above all compiled an inventory of the issues and considered the scope and/or depth in which they should be dealt with by the expert group and did not, therefore, make any concrete proposals for action. The establishment of an international court for cybercrimes did not appear on the extensive agenda.

  On the one hand, the comprehensive approach of the initiative is to be welcomed, on the other hand, there is the obvious danger that the expert group will be occupied for years making an inventory and that the production of concrete proposals will fade into the background.

- ***EU – US "Working Group on Cybersecurity and Cybercrime"***

  The United States and the European Union established a "Working Group on Cybersecurity und Cybercrime" in November 2010 in Lisbon to develop a cooperation programme and a roadmap, including the development of common approaches to various problems in Internet criminality and Internet security as well as a cooperation and practice in critical Cyber incidents[14], and the development of Public-Private Partnership Models for cooperation between government institutions and industry in the establishment of Internet security and combating Cyber criminality.[15] The task of advancing the Council of Europe (COE) Convention on Cybercrime and encouraging EU and pending EU and CoE Member States to rapidly become parties is especially important (at best before November, 2011).[16] The explicit call to combat child pornography and the fact that Germany and the USE intend to coordinate their positions in the UNODC Cybercrime Expert Group are especially worthy of mention.[17] Even though the working group has not so far been able to present any results, its objectives seem to be concrete and achievable.

---

[13] of 17.-21. January 2011 in Vienna
[14] Concept Paper of the EU-US Working Group on Cyber-Security and Cyber Crime, April 2011, p. 1 [EU-US WG Concept Paper 2011]
[15] EU-US WG Concept Paper 2011, p. 2
[16] EU-US WG Concept Paper 2011, p. 4
[17] EU-US WG Concept Paper 2011, p. 4 u. 5

- ***EastWest Institute Cybercrime Legal Working Group: Initiative for an International Cyber crime court***

  An international court for cyberspace (ICTC) is suggested by the Norwegian judge Stein Schjolberg, who considered the subject in the context of the Cybercrime Legal Working Group of the EastWest Institute (EWI) ().[18] The members of the working group are independent and non-governmental experts for Internet security and Internet criminality and the working group has the task of making recommendations for new legal methods to combat Internet criminality and Cyber attacks.

  Stein Schjolberg proposes in his paper[19] that an ICTC be instituted as a subsection of the International Criminal Court, and be based either in The Hague or in Singapore. Schjolberg is of the opinion that the ICTC would, with this structure, be covered by the Rome Statute which provides for all institutions for investigation and criminal prosecution which the court would need. The public prosecutor could, as an independent organ of the court, commence investigations including on extraordinary grounds.

  Alternatively, an ad-hoc court could be considered. That would have to be a court of the United Nations established by a resolution of the UN Security Council in accordance with Chapter 7 of the UN Charter. Schjolberg quotes the International Criminal Tribunal for the former Yugoslavia (ICTY) as a model. The Tribunals jurisdiction would be prosecuting and punishing cybercrimes, and should cover the following issues:

    - violations of a global treaty or set of treaties on cybercrime
    - massive and coordinated global cyber attacks against critical information infrastructures.

  The Tribunal would have concurrent jurisdiction in relation to national courts, but may claim primacy over national courts and take over investigations and proceedings at any stage. In the vision of the ICC, an International Criminal Court for Cyberspace would 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 an exceptional basis.

  Although the court prosecutor would have wide-ranging powers and must, of course, have corresponding qualifications, it is clear that he/she would not have the capacity alone to effectively conduct investigations for the ICTC. Schjolberg therefore proposes close cooperation with INTERPOL which, since the 1980s, is accepted as the leading institution with knowledge of the investigation of international Cybercrimes. Since 1990, regional working groups for Africa, Asia/South Pacific, North and South America, Europe, the Near East and North Arica have been

[18] Das EastWest Institute (EWI) was founded in 1980 in order to enable individuals, institutions and nations to communicate through a network across the borders of the Iron Curtain. It is a „think-and-do-tank“, developing innovative solutions for urgent security problems and implementing them. Many prominent personalities from politics and industry are members.

[19] Stein Schjolberg: An International Criminal Court or Tribunal for Cyberspace (ICTC), May 2011, www.cybercrimelaw.net [= Schjolberg 2011]

set up at INTERPOL, the leaders of which are experienced members of national units for combating computer criminality.

At present, INTERPOL is working to establish Interpol Global Complex (IGC) in Singapore expected to be in full operation in 2013/2014 with a staff of about 300. The ICG will concentrate on the development of innovative and state-of-the-art policing tools for worldwide law enforcement especially in enhancing preparedness to effectively counter cybercrime. The IGC will therefore be an extremely important initiative for international law enforcement against Cyber criminality.[20]

Schjolberg also proposes the establishment of a Global Virtual Taskforce consisting of experts in the global information and communications technology industry, financial service industry, non-governmental organizations, academia, and global law enforcement through INTERPOL, working in partnership, will be necessary for the prevention and effective combating of global cybercrimes, especially for delivering fast time responses to cyber attacks.[21]

Schjolbergs proposal for the establishment of a court is very detailed – he has even provided a draft UN resolution and a draft of statutes for the court. However, his ideas almost completely ignore the work of other initiatives – although he mentions them briefly at the beginning.

6. Diversion: The Problem of Identifying the Perpetrator and Collecting Evidence

Before commenting in principle on the initiatives introduced, a fundamental problem of Cyber criminality must be addressed. Due to the technological environment in which they are committed, it is extremely difficult to investigate Cybercrimes. Undetected hacking enables Internet criminals to perpetrate their acts without fear of early detection, not to mention arrest and criminal prosecution.[22] It seems that cyber criminals are developing new techniques at a pace which even the most sophisticated technology cannot match.[23] For this reason, a naturally unknown but estimated great number of Internet crimes are simply never discovered.[24] The more organised and developed an attack is, the more difficult it is to detect and punish.

Sandro Gaycken[25], security researcher at the FU Berlin, lists four factors which in his view render the investigation and punishment of cyber crime almost impossible and therefore question in principle the usefulness of a cyber criminal law – and naturally therefore an international court:

- *The fluidity of physical clues*: The relative miniscuity of the attack (e.g. an infected USB stick) means that almost no physical traces of the attacker remain. And that applies even more so to attacks through the Internet.

- *The "narrative" character of the hostile programme:* This means that the attack code itself is deliberately designed (in a language) and the design can also be used to mislead investigators as to the origin of the code.

[20] Schjolberg 2011, p. 17
[21] Schjolberg 2011, p. 17/18
[22] Deloitte Center for Security and Privacy Solutions: Cyber crime: a clear and present danger. White Paper, 2010, p. 4 [= Deloitte White Paper 2010]
[23] Deloitte White Paper 2010, p. 5
[24] Deloitte White Paper 2010, p. 6
[25] Sandro Gaycken, Krieg der Rechner, in: Internationale Politik, März/April 2011, p. 88-95 [=Gaycken 2011]

- *The man-machine gap*: The gap between man and machine has the result that even if an attack can be traced back to a certain computer, this says nothing about who was using that computer at the relevant time and what his motives were.

- *The universality of the weapons in the cyber war*: Over-the-counter technology in computers, standard USB sticks or common programmes are used, bad intentions cannot be deduced from programming expertise. No "murder" weapon can therefore be found.[26]

  Another issue also complicates the investigation. Authors of hostile programmes and other cyber criminals are "for hire", providing their abilities, opportunities and products to the beneficiary of the crime for cash.[27] This kind of criminal activity can be compared to that of the contract killer – although a serious crime is committed, there is no personal motive resulting in prolonged investigation before the "executioner" is found.

  The "non-attributability" of cyber crimes resulting from the above factors, is widely discussed among experts at present.[28]

  It is equally true that forensic IT is working under immense pressure on solutions to these problems and that some successes can be claimed. New research on IT forensic design aspects of a secure computer architecture concentrate particularly on the problem of securing evidence traces, a core problem of identifying perpetrators and substantiating evidence.[29] It cannot, nevertheless, be denied that – at least to date – security and prosecution methods are lagging far behind the perpetrators.

7. Assessment and Conclusion

Almost all significant initiatives on international law enforcement in Cybersecurity and Cybercrime originated in 2010 and 2011.[30] Even though varying in range and sometimes partially complementary, the lack of coordination is striking. This is a cause for concern when one considers that the aim of the initiatives is precisely an improvement in international cooperation even as far as united action. Today, a great deal of parallel work is evident with consequent major exertions in consultation and coordination of results awaiting the working groups. The initiative of the UNODC in particular clearly harbours the danger of submersion in stock-taking. A positive aspect is that all initiatives intend to involve the private sector – the need for cooperation not only across state borders but across all institutional borders is unquestioned. All initiatives acknowledge that a purely legal approach to the problem of Cyber crime offers no solution.

It is noticeable and regrettable that so far none of the initiatives have addressed the problem of "non-attributability".

---

[26] Gaycken 2011, p. 91-94

[27] Deloitte White Paper 2010, p. 5

[28] e.g. the Auswärtige Amt, in cooperation with the FU Berlin and UNIDIR, plans a conference on „Challenges in Cybersecurity" for December 2011. Various panels – one chaired by Prof. Sylvia M. Kierkegaard – will discuss the problem of non-attributability.

[29] cf. e.g. Klaus Hildebrandt, Stefan Hummel, Igor Podebrand, IT-Forensik. Ausgewählte Aspekte zu Sicheren Rechnerarchitekturen, FAT und NTFS, Berlin 2011. It is noted that this work takes up all aspects which the above mentioned Deloitte Study refers to as causes of undiscovered Cyber attacks.

[30] The activities of the International Telecommunication Union, a UN organisation, published with the American Bar Association in 2009 a 69 page „Toolkit for Cybercrime Legislation". cf. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf

For the great majority of the commentators, the Cybercrime Convention of the Council of Europe is the best basis at present for creating an international legislative framework. 47 states have already become parties including four (very important) non-EU members, namely, the United States, Canada, Japan and South Africa. The extensive cooperation requirements to which the parties are subject are also regarded as a promising basis for international law enforcement.[31] The Convention is also supported by the Asia-Pacific Economic Cooperation, the European Union, INTERPOL and the Organisation of American States.[32] Nevertheless, states which were not involved originally in drafting the Convention have understandable reservations about joining. It may be possible to relieve these reservations by granting new signatories rights of participation in the further development of the Convention.[33]

The fundamental difficulties in achieving a single international standard – namely the discrepancies between the western countries and the developing nations, the fundamental rejection of the BRIC states[34], widespread reservations against interference in state sovereignty – would be all the more evident in a complete restart of negotiations. In addition, new negotiations extending over years would presumably delay the implementation of existing reform projects considerably.[35] It does not therefore seem useful at present to start new negotiations from scratch.

Even if there may be controversy about its structure to a greater or lesser extent – no one now doubts the necessity of an international legal framework. If this were established, an international court could also function effectively. It would not, however, be the court as the EWI Working Group led by Stein Schjolberg sees it.

Presumably, to shorten the very prolonged – not doubted - process towards achieving international agreement on the prosecution of cyber crime, Schjolbergs ICTC would be linked, by resolution of the UN Security Council, to the International Criminal Court. Since that court is covered by the Rome Statute, it (and therefore the Cybercrime Court) has jurisdiction only for the most serious crimes (war crimes and crimes against humanity), to which e.g. child pornography crimes would not belong. Cybercrimes are, however, – even though terrorist and warlike attacks of course, occur, which must also be pursued - above all *transnational economic crimes*. With such a drastic limitation of the crimes covered, as proposed by Schjolberg, the Cybercrime Court would not have the jurisdiction to deal with the international problems which must undoubtedly be tackled.

The other obstructions which the international Criminal Court faced and to some extent still faces would also be in the way [36] including that especially important states, such as the United States have still not recognised the International Criminal Court. With China and Russia, two other of the five permanent members of the Security Council are also missing.[37] A court based on the ICC would be weighed down by this burden from the outset.

Based on the information available at present, it could be a possibility that the Council of Europe establishes a court with jurisdiction for adequately serious transnational crimes committed in or from a

[31] Brian Harley, A Global Convention on Cybercrime?, March 2010, p. 3 [= Harley 2010]
[32] Harley 2010, p. 4
[33] Harley 2010, p. 4
[34] Brazil, Russia, India and China
[35] Harley 2010, p. 4
[36] cf. lecture of Gregor Schirmer, Vom Internationalen Militärtribunal zum Haager Internationalen Gerichtshof – Fortschritt und Ernüchterung, 12.10.2010 [= Schirmer 2010]
[37] Schirmer 2010, p. 12

signatory state. The existing legal harmonisation methods and mutual legal assistance practice could be usefully supplemented by such an institution. An adequate number of signatory states would, of course, be necessary and therefore an amendment of the Convention in accordance with the requirements of new members – initiatives in this direction are already being taken – and a practicable and clear identification of crimes which the court could investigate and punish.[38] With this structure too, harmonisation of international law and the establishment of the international court would be running not only parallel but even hand in hand. The members and new signatories could agree in the expansion process on the structure and jurisdiction of the court.

A further argument for this connection would be the explicit support of the Cybercrime Convention by INTERPOL. As Stein Schjolberg rightly argues, this institution is the one best equipped to support the investigation and prosecution of crimes by the International Cybercrime Court.

With an expanding number of signatory states and the establishment of the court at the same time, two main problem areas would have to be closely monitored, firstly, the differing legal understanding particularly of Intellectual Property, which the European Council explicitly included in the Convention and which scared off a number of states from joining, and secondly, the degree to which the states must surrender sovereignty in submitting to judgements of the court – a significant reason why, for example, the United States has not recognised the International Criminal Court in The Hague. Both aspects certainly constitute major obstacles the surmounting of which is likely to take some time.

8. The establishment of a WCLF Working Group for the International Court for Cybercrime

There are a number of points of contact in favour of cooperation of the WCLF and, after appropriate preparation, the Global Law Society. Firstly, the establishment of a working group to further consider and prepare concrete proposals for an *International Court for Cybercrime* linked to the Council of Europe is indicated. This working group could undertake the following tasks:

- Specifying the conditions which must be fulfilled by a court based on the Cybercrime Convention.
- Proposals for the development of a Collective Code (further development of the Cybercrime Convention with the participation of many states).
- Identification of Cybercrimes for which the court would have jurisdiction.
- Reviewing the status of the judgements (subsidiary or with priority over national judgements).
- Concrete ideas on the structure of the court (institutionally, personnel, finance)
- Contribution of ideas to the various ongoing initiatives
- Preparation of lobbying proposals
- Acquisition of further supporters.

[38] All crimes against society (cf. list at 1.) should be included in any event.

The members of the working group could include the following:

WCLF:

Prof. Dr. Sylvia M. Kierkegaard, LL.M, LL.B, Southampton, Chair

External experts (in alphabetical order):

Prof. Dr. Susan W. Brenner, Dayton

Dr. Sandro Gaycken, Berlin

Prof. Dr. Dr. Eric Hilgendorf, Würzburg

Dr. Françoise Le Bail MSc, General director EU Commission, Brussels

Prof. Dr. Alexander Lorz LL.M, Düsseldorf

© WCLF 2011