United Nations A/CONF.213/IE/6

Twelfth United Nations Congress on Crime Prevention and Criminal Justice

Salvador, Brazil, 12-19 April 2010

Distr.: General
22 March 2010

Original: English

Items 8 of the provisional agenda*

Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime

Background documents** received from individual experts***

CYBERSPACE OR SOVEREIGN STATES ?

Prepared by

Henrik S. Spang-Hanssen

Citation:
Henrik Spang-Hanssen, Cyberspace or Sovereign States (22 March 2010), Presented at 12th UN CPCJC Congress, Salvador 12-19 April 2010, Brazil. UN doc A/Conf.213/IE/6.
Available at SSRN: http://ssrn.com/abstract=1582645

* A/CONF.213/1.

** Distribution is limited to the quantities and languages in which the paper is made available to the United Nations Office on Drugs and Crime.

*** The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Please recycle

CYBERSPACE OR SOVEREIGN STATES ?

Presented to
The Twelfth UN Congress on
Crime Prevention of and Criminal Justice
Salvador, Brazil, 12-19 April 2010

by

Henrik S Spang-Hanssen,[1] *Independent Senior Researcher*
(formerly Prosecutor and Supreme Court Attorney-at-law in Denmark)

Silicon Valley, California, USA
hssph@yahoo.com
http://hssph.net

[1] Author of among other things: **The Future of International Law: CyberCrime** (2007)(available from the Social Science Research Network's (SSRN's) Working Paper Series at http://ssrn.com/abstract=1090876); **A Just World under Public International Law in Cyberspace: Jurisdiction** – Chapter 1 to "CYBER JURISPRUDENCE" (Icfai University Press, 2008); **Cybercrime Jurisdiction in Denmark** - Chapter 8 to: CYBERCRIME JURISDICTION: A GLOBAL SURVEY (T.M.C. Asser Press , 2006); **Public International Computer Network Law Issues** (Chapter 7 on cyber crime)(DJØF Publishing, 2006); **Cyberspace & International Law on Jurisdiction** (DJØF Publishing, 2004), Cyberspace Jurisdiction in the US - The International Dimension of Due Process (Norwegian Research Center for Computers and Law, 2001).

A longer and more descriptive title would be:

> "Global Jurisdiction over Cyberspace acts is allowed for all nations, there is no limitation to the exterritorial reach / range of national jurisdiction. Thus, as far as computer-related crimes are concerned, there are no sovereign states!
>
> OR
>
> Does the international community STILL want to be divided into sovereign states when computer-related crimes are at issue? If so, all nations must accept that whatever a cybernaut does legally on a computer in his/her own country, under that country's constitution and laws, means that he/she cannot be charged or indicted for such acts in foreign countries.

1. Introduction

Ten years of extensive research on the subject of jurisdiction and public international computer networks ("the Internet") can be summarized as follows:

In the beginning of the 1990's, the courts in the United States had huge problems figuring out how to decide which of the 50 federal states had jurisdictional over a specific Internet-related case.[2] Overall, U.S. cases only involving online facts have been decided on the basis of whether the particular court could find a (close) link[3] between the out-of-state defendant and the Internet activity (and whether it would be just and fair to require the defendant to be subjected to – for him/her – "foreign" jurisdiction).[4]

Naturally, similar – if not larger – problems exist between the countries of the world, as what is involved is not simply federal states under one constitution but sovereign states, each with its constitution or similar basic rules.

At the start of the new millennium, attempts were made in The Hague to draft a treaty for jurisdiction and enforcement in civil law matters related to the Internet. However, these discussions stalled because of disagreements on basic principles between the E.U. and U.S.[5]

In 2001, the European Council introduced (after discussions with the U.S. and Japan) a draft to a CyberCrime Convention.[6] However, the drafting committee neglected a vital, specific issue, namely "Task V" to solve:

> ***"the question of jurisdiction in relation to information technology offences, e.g. to determine the place where the offence was committed (locus delicti)*** and which law should accordingly apply, including the problem of ne bis idem in the case of multiple jurisdictions and the question how to solve positive jurisdiction conflicts and how to avoid negative jurisdiction conflicts;"[7] (*my emphasis*)

---

[2] HENRIK SPANG-HANSSEN, CYBERSPACE JURISDICTION IN THE US - THE INTERNATIONAL DIMENSION OF DUE PROCESS (CompLex 5/01, Norwegian Research Center for Computers and Law 2001). Also available from Social Science Research Network (SSRN) at http://ssrn.com/abstract=1105703 [hereinafter SPANG-HANSSEN-1].

[3] Compare the issue of a "link" in the *ICJ Nottebohm case (Liechtenstein v. Guatemala)*, 1955 I.C.J. 4 (6 April 1955, Second Phase). See also sections 31.2.2.2. and 32.1 on "sufficient closeness" in HENRIK SPANG-HANSSEN, CYBERSPACE & INTERNATIONAL LAW ON JURISDICTION pages 371-372 & 389-425 (DJØF Publishing, 2004) [hereinafter SPANG-HANSSEN-2].

[4] Henrik Spang-Hanssen, *Website Cases Survey Result: The Zippo Decision is Still the Leading Case - If the Decision is Used Faithfully* (2008). Available from Social Science Research Network at http://ssrn.com/abstract=1114745.

[5] See, SPANG-HANSSEN-2 *supra* note 3, at 453-460 (Section 33.5. Draft to a Hague Convention).

[6] The (European) CyberCrime Convention of 2001 (or "Budapest Convention") - ETS no. 185 of 23 November 2003 (entered into force 1 July 2004) at http://conventions.coe.int/treaty/en/treaties/html/185.htm. Chart of signatures and ratifications, Council of Europe at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=10/03/2010&CL=ENG (last visited 9 March 2010).

[7] Section II. The preparatory work, No. 11.v of Explanatory Report to Convention on Cybercrime (ETS No. 185) http://conventions.coe.int/Treaty/en/Reports/Html/185.htm (last visited 9 March 2010).

*****

I claim: Before the jurisdictional question is solved – no real cybercrime convention can be drafted.

Or: How can anyone discuss the issue of "cybercrime" – whatever that word/term shall cover as to crimes - BEFORE one has established the jurisdictional LIMITS/BOUNDARIES for criminal legislation – OR alternatively decided to ALLOW each and every state on the planet to exercise GLOBAL jurisdiction over ALL cybercrimes!

Today's children and adults employ computers constantly. Children use computers to learn, experiment and play. Adults utilize computers in many aspects of life, for instance, communication with friends and government, exchange of opinions, online banking, etc.

As most acts done on the Internet involve cross-border transmissions, the effects of a citizen's computer use can be felt both domestically and in a foreign country. This implies that not only national law but also foreign law is involved.

At least adults are expected to know the law of their own countries.

However, some use of computers can also - unknowingly - imply/mean violation of foreign laws. This is to a large degree due to an unsolved matter in public international law related to Cyberspace - the jurisdictional question, that is, where is(are) the relevant place(s) where things happen when using the Internet and, thus, ultimately, which law(s) applies(y).

The following section will provide some scenarios, which are the sum of many situations that have occurred in the past or will likely occur in the future. The scenarios are not exercises in paranoia, for they are not far-fetched and they accurately illustrate how different countries deal with Cyberspace.

2. Scenarios

A journalist JOL working for a small purely online newspaper HERALD in the federal state SUB in State A writes a small article in English about a statement politician POL has made about journalist SUE also working for a newspaper in SUB. SUE asserts that the statement is untrue/false. SUE's attorney finds out that the statement is illegal under the criminal law in State B – located on another continent - and that the damage awards are much higher in State B than under the laws of State A and SUB. State B does not have any requirement that a case - as in State A - should be dismissed if exercise of jurisdiction would not be an exercise of fair and substantial justice. The jurisdictional rule in State B only specifics that there must be a link or connection between the defendant and English-speaking State B.

The court in State B accepts the case filed by SUE's attorney against the politician POL because State B's citizens can read the newspaper article online; accordingly, there is a sufficient jurisdictional link. The court rejects POL's attorneys argument that the case is between two citizens of SUB (and State A) such that the case should be dealt with by courts in SUB or State A and that the article was only intended for the newspaper's local audience in SUB The court holds POL's statement is false and therefore finds POL has violated the criminal code in State B. It imposes a penalty on POL equal to $50,000. Further, the court awards SUE the equivalent of $150,000 in damages.

Because POL does not pay the penalty, State B forwards the court decision to state SUB, where POL's attorney argues that the court should dismiss the case as POL has not gone beyond the limits of what is permissible under the SUB constitution's free-speech provisions. The court in SUB agrees with POL's attorney and rejects enforcement of the court-decision from State B, which – in turn – thereafter issues an arrest warrant over POL.

POL's attorney informs his politician client POL that he can no longer travel to the continent where State B is located due to an arrest-warrant-extradition treaty-system between the states on that continent.

Meanwhile, SUE's attorney realizes that some people – in the small fishing-harbour-town located in State C on another continent where SUE has a small cottage and spends a few weeks each year for summer vacation – have also read the article online. SUE's attorney files a lawsuit against newspaper

HERALD and journalist JOL for damages in the local court in State C. This court holds it can exercise jurisdiction, as some of its citizens have read the article. It awards SUE an amount equal to $25,000 in damages. It also rejects POL's attorney's argument that the case is between two citizens of SUB (and State A) such that the case should be dealt with by courts in SUB or State A and that the article was only intended for the newspaper's local audience in SUB. Furthermore, the court rejects the attorney's argument that the article is protected by a free-speech and freedom-of-the-press provision in State A's constitution. Indeed, the court holds it has jurisdiction over whatever its citizens are able to read on the Internet, even though the article was written in English, which is not the language used on the continent where State C is located.

However, state SUB also rejects enforcement of the court decision from State C. Thus, SUE does not receive any money out of the two foreign-court decisions granting her claims for damages, and she still has to pay her own attorney fees.

Elsewhere, Ahmed, a 15-year-old, is somewhat of a computer nerd. He invents a software program that should be able to retrieve forgotten passwords. He tests the software on his own and his father's computers and it seems to work.

Ahmed tells one of his co-workers at a supermarket, Enrico – who is over 18 – about the software. Enrico copies the software from Ahmed's laptop while it is unattended. Enrico likes to hack into computers just to find out whether he can bypass firewalls, etc. He uses Ahmed's software to hack into foreign state CDONU's military computer network. Enrico never intends to destroy or copy anything. However, in this instance he cracks some parts of the CDONU military's systems, due to an unintended feature in Ahmed's software. The CDONU military notifies the police about the break-in. The police discover that Enrico has copied Ahmed's program and require that Enrico and Ahmed be extradited for prosecution.

Neither Ahmed's nor Enrico's country is a party to this convention.

In another location, a woman belonging to a criminal gang approaches a 14 year-old girl, Tania, in a public library and asks her whether she wants to earn $100 by connecting a USB flash-drive stick to one of the public library's computers and pressing an "OK" button when it appears on the screen. The woman explains that she is not personally confident in using computers. Tania accepts the offer, inserts the USB stick, and clicks "OK" on the screen, which next states that "all is well and the program will now shut down itself." What actually happens is that the clicking of the OK button initiates a program that starts copying several stores' credit card data, which is then transmitted to the criminal gang's computer in foreign country Charge. Tania's country is not a party to the CyberCrime Convention.

In the meantime, Ahmed's government rejects the request it has received to extradite him to the foreign country CDONU as he has not violated any national law in his own country and is a minor.

Enrico has not violated any national law in his own country. The foreign country CDONU nevertheless demands his extradition for having violated its criminal code on national security. Enrico's attorney brings the government's decision to extradite him before the courts. On appeal, the supreme court of Enrico's country decides to allow the extradition. However, the court adds conditions to the extradition, namely that any jail sentence imposed cannot exceed the maximum limit for similar national security codes in Enrico's country (twenty years) and, further, that the sentence has to be handed down at one time in total for all the offenses found by the court in CDONU.

A jury in CDONU finds Enrico guilty of three charges, which verdict would normally carry a sentence of three times sixty (i.e., 180) years in jail pursuant to the CDONU criminal code, with a right to parole after two-thirds of the time is served. However, the court in CDONU reduces the jury's sentence to twenty years due to the extradition conditions attached by Enrico's country.

Tania's local police, meanwhile, find she did not have any intent to violate any law and determine not to press any charges. However, country Charge requires Tania to be extradited and her country's government authorizes extradition due to an existing bilateral extradition-treaty. A jury in country Charge then finds Tania has violated its criminal code pursuant to which it is a crime to copy credit card information from a database. The code has a "Three Strikes Rule," under which the minimum sentence of imprisonment is 25 years. The jury finds seven databases have been copied and that the Three Strikes Rule should be used. Tania is sentenced to 25 years in prison.

3. Comments

The above illustrates how easy an act done on a computer becomes an issue in foreign courts and/or a foreign crime. Again, the scenarios are not exercises in paranoia. They are true to the facts of real-life cases that have already occurred.[8]

So the above illustrates how different countries deal with violations done with use of computers. In many cases, the violators – whether minors or adults – have no idea of in which countries they can be indicted/charged, tried, convicted, sentenced and imprisoned ... and thus no inkling of how long their confinement can be. There is no predictability because the international community has not yet decided neither where, that is in which state, the criminal computer act has been initiated and done/executed nor in which places and which courts there is jurisdiction to adjudicate.

Thus, first of all, the most vital – and basic – question for Cyberspace must be solved, namely *"where is the place?"*

It is computer technology that has created this new, thorny situation, not legal rules, that were made long before the invention of international computer networks that both allow worldwide access to information and disregard any national borders/circumvent any obstacles in the network. Now, when dealing with the sea or the air, it is a fact of physics that a ship or airplane cannot be everywhere at the same time. Yet Internet websites can be looked and acted upon from many places at the same time. This fact can make it – unlike the situation in maritime law and aviation law – extremely difficult to determine where the "actual (legal) location" is.[9]

It is essential to provide time for thorough consideration of this issue. It seems far into the future that we will be able to say that sufficient research and knowledge on the legal aspects and the technology has been achieved.[10] Retired U.S. Supreme Court Associate Justice Souter remarked in a case[11] that "we should be shy about saying the final word today about what will be accepted as reasonable tomorrow.... In my own ignorance I have to accept the real possibility that ... if we had to decide today ... just what the First Amendment should mean in cyberspace ... we would get it fundamentally wrong."

3.1. Global Jurisdiction

To date, many courts in different countries – when confronted with computer/Internet crimes – have exercised what could be called "Global Jurisdiction"[12] – and basically have attempted to indict any computer user on earth if the particular country's criminal laws embraced the act as a violation.

I have labeled this approach with the term "Global Jurisdiction," which is characterized by a State's jurisdictional rules being taken on its "wording" to reach all alien cybernauts, thus conferring jurisdiction involving aliens outside the forum state anywhere in the world.

Such a state of affairs is clearly an unreasonable regime, given that it requires any individual user of the Internet to know the laws of all of the sovereign states on the planet. Another former U.S. Supreme Court Associate Justice, Sandra Day O'Connor, has pondered:[13] "why judges and lawyers should divert their attention ... to the principles and decisions of foreign and international law. The reason, of course, is globalization. No institution of government can afford any longer to ignore the rest of the world."

---

[8] See, for example, cases dealt with in Chapters 21 & 34 in SPANG-HANSSEN-2 *supra* note 3, and HENRIK SPANG-HANSSEN, PUBLIC INTERNATIONAL COMPUTER NETWORK LAW ISSUES pages 203-279 (DJØF Publishing, 2006) [hereinafter Spang-Hanssen-3].

[9] Henrik Spang-Hanssen, *Filterblokering af websiders indhold og lovgivning af Internettet - herunder Yahoo-sagen [Filtering and Blocking of Websites' Content and Legislation on the Internet - Including the Yahoo Case]*, KRITISK JUSS (Norwegian Law Journal - Critical Law), No. 3-4, pp. 321-328 (2001). English translation available at Social Science Research Network at http://ssrn.com/abstract=1092384.

[10] *Id.*.

[11] *Denver Area Educational Telecommunications Consortium, Inc. v FCC*, 518 U.S. 727, 777 (U.S. 1996).

[12] SPANG-HANSSEN-3 *supra* note 8, at v, Foreword; Henrik Spang-Hanssen, *The Future of International Law: CyberCrime* at section 3.1 (2007)(available from the Social Science Research Network's (SSRN's) Working Paper Series at http://ssrn.com/abstract=1090876.

[13] At the Southern Center for International Studies, Atlanta, Georgia, 28 October 2003 (available at http://workersrights.humanrightsfirst.org/us_law/inthecourts/SOUTHERN_CENTER_INTERNATIONAL_STUDIES_Justice_O'Connor.pdf) (last visited 18 March 2010).

4. Each State Party will exercise its rights and fulfill its obligations under this Convention to the extent practicable in accordance with the following priority of jurisdiction:

- first, the State Party in which the alleged offender was physically present when the alleged offense was committed;
- second, the State Party in which substantial harm was suffered as a result of the alleged offense;
- third, the State Party of the alleged offender's dominant nationality;
- fourth, any State Party where the alleged offender may be found; and
- fifth, any other State Party with a reasonable basis for jurisdiction.

Thus, the drafters' intention with the Stanford Proposal was to avoid multiple-state jurisdictional conflicts by limiting its scope to cyber activities that are universally condemned.

This would safeguard protection of the individual cybernaut and "regain" the cybernaut's fundamental human rights.

However, the Stanford Proposal also includes the following:

3. This Convention does not exclude any criminal jurisdiction exercised in accordance with domestic law, including any domestic law giving effect to Articles 3 and 4, or any criminal jurisdiction established pursuant to any other bilateral or multilateral treaty.

Thus, this part 3 of article 5 is somewhat of a step backward in relation to parts 1-2 and 4 as regards the individual cybernaut, because part 3 allows an individual State-party to continue to decide what its exterritorial jurisdictional reach shall be – beyond what the international community determines.

Thus, the Stanford Proposal really does not forbid a State's courts – when crimes have been committed by use of the Internet – from exercising what could be called "Global Jurisdiction" and indicting any computer user on Earth.

And this continues to imply an unreasonable regime that requires any user of the Internet to know the laws of all states on Earth.

As for the CyberCrime Convention of 2001, its main problem is that subsections (a) through (c) of section 1 of Article 22[17] do not determine when something related to Cyberspace is occurring "in" or "on" the territory. Because computer technology is new, public international law has not developed any standard practices concerning when a Cyberspace-act is occurring "in" or "on" a territory. As stated previously, this is probably the most difficult and most controversial issue in Cyberspace law, and it is an issue that the drafting committee – as the "steppingstone" – ought to have resolved before drafting any other articles.[18]

To repeat, we need a truly international Internet Crime Convention that prevents Internet users from being indicted in foreign countries for violations they were "rightfully" not aware of.

To this end it is important to remember that a cybercrime convention:[19]

- As a first base, should only deal with pure online ("cross-border") issues. That is, no cross-border physical shipments or tangible things are involved; at least one user is a foreigner, that is, a nonresident or non-national in the State or court in question -- Transportation (physical items) ↔ Transmission (bits - electronic)
- A second base to remember is that no one owns Cyberspace. The Internet can, and should, not belong to any single State or special group of States. The public international computer network is something "given to mankind."
- A third base is: no worldwide or Global Jurisdiction[20] besides Universal Jurisdiction. Universal Jurisdiction is, as observed above, only permitted when the international community has accepted it for a LIMITED and SPECIFIC issue such as war crimes or piracy.

---

[17] See Appendix 1 in the back.

[18] SPANG-HANSSEN-3 *supra* note 8, at 318; and HENRIK SPANG-HANSSEN-2 *supra* note 3, at 296-462.

[19] Further on "Henrik's Six Steppingstones," see SPANG-HANSSEN-3 *supra* note 8, at 1-8. A short outline at http://hssph.net/Henriks6Steppingstones.pdf.

[20] "Global Jurisdiction" – a statute taken on its "wording" reaches all alien cybernauts who can be anywhere in the world.

Legislation for cyberspace/computers must occur at other layers than the IP/TCP-layers in the network.[30] One of the inventors of the Internet Protocol Suite stated in the French Yahoo! case – as to the court requiring filtering on the Internet – that "if every jurisdiction in the world insisted on some form of filtering for its particular geographic territory, the World Wide Web would stop functioning."[31]

Therefore, a necessary "steppingstone" for writing code on jurisdiction of Cyberspace is that lawyers from different countries -- whose citizens uses public international networks – (and possibly after each has conferred and verified with his/her parliaments/politicians) -- find some common denominator in the shape of one set of rules that expresses the highest possible consensus between the different countries.[32] Thereafter, the lawyers will be able to explain to the computer technicians how the common denominator-rules are thought to work and to expound the thinking behind them.[33]

3.3.1. Sufficient Closeness

On public international networks, every State could be said to possess concurrent jurisdiction, since the online experience in every State will be the same for everybody; thus, the "effect" will be everywhere. Therefore, in terms of Cyberspace, it seems more appropriate to use the term "closeness" than "effect" or "target."

Now, the real problem of international law is to define the circumstances in which the relevant points of contact (the legal relationships)[34] are sufficiently close.[35] When dealing with jurisdiction to prescribe, it should be remembered that in international law jurisdiction does not mean determining whether another State has an equally close or a closer – or perhaps the closest -- contact, as concurrent jurisdiction is allowed.[36] Nevertheless,, international law principles do not allow every State to have jurisdiction to prescribe.[37]

3.3.2. Fair Play & Substantial Justice

The international dimension of due process in the cyberspace environment must contain both reasonableness and predictability/foreseeability.[38]

A plaintiff's attempt to forum shop because of a likely better litigation result in a foreign court, as opposed to a closer and more obvious one, should not be considered "fair play and substantial justice."

In international law, the principle of reasonableness appears unobjectionable, so long as it is understood that mere political, economic, commercial or social interests are to be disregarded when it comes to the weighting that every respected judicial test of reasonableness implies. Further, it is reasonableness in public international law that is decisive. In each case the overriding question is: Is there a sufficiently close legal connection to justify, or make it reasonable for, a State to exercise jurisdiction? Exercise of jurisdiction by more than one State may be reasonable, because public international law does not prohibit concurrent jurisdiction over international criminal and civil matters. However, a State should defer to another State if that latter State's interest is clearly greater. It is reasonable to require of any State that it acts in such a way that gives a degree of predictability to the legal system that allows potential defendants to structure their primary conduct with some minimum assurance as to where that conduct will and will not render them liable to suit.[39]

---

[30] An overview of the computer network layers is printed as Table 2.6 in SPANG-HANSSEN-3 *supra* note 8, at 56.

[31] Vinton Cerf in *Top Internet advisor criticizes French Yahoo! Decision*, 24 November 2000, AGENCE FRANCE PRESS, 2000 WL 24767154 (Westlaw database AGFRP).

[32] But this necessary initial step was not even possible to achieve at the Hague Conference on Jurisdiction and enforcement over a period of 10 years. However, it might be that limiting the issue to only pure on-line incidents could break the ice.

[33] SPANG-HANSSEN-2 *supra* note 3, at 519-522.

[34] F.A. MANN, *The Doctrine of Jurisdiction in International Law*, 111 RECUEIL DES COURS 1, 44 (1964-I).

[35] *Idem* at 83.

[36] *Idem* at 46, 49 & IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 301 (5th Edition, Clarendon Press, Oxford) (6th Ed. Page 297).

[37] SPANG-HANSSEN-2 *supra* note 3, at 365-366 & 382-418.

[38] SPANG-HANSSEN-2 *supra* note 3, at 369-371 & 418-425.

[39] SPANG-HANSSEN-3 *supra* note 8, at 169-170.

3.3.3. A Framework

In my opinion, the crux of the above should be that jurisdiction can be exercised in the following situations:

- **The State to which the cybernaut is a citizen;**
- **The State in which the cybernaut is a permanent resident;**
- **The State in which the "involved" computer was hooked up to the Internet and the uploading or downloading took place;**
- **The State that, pursuant to the cybernaut's Internet service provider agreement, has been chosen to be forum; or**
- **As for "exterritorial" jurisdiction: the State or States (but only a handful that are predictable for the cybernaut) where there exists sufficient closeness between the cybernaut and the State in question (for example, where the "effect" occurred/happened[40]) and it would not be against fair play and substantial justice to require the cybernaut to submit to the jurisdiction of a foreign court.**

This would provide a much more predictable and secure environment for cybernauts and prevent them from being sued in States that only have weak connections to them.

At the same time, this would be a fair restriction/limitation of any State's exterritorial jurisdiction, which properly never was intended to embrace cases that only the Internet has recently made technically possible. Furthermore, it would reduce the risk of some States' courts being overloaded because of plaintiffs' forum shopping.

Such a regime would secure the individual cybernaut his human rights -- establishing once and for all that whatever a cybernaut does legally in his/her own country under that country's constitution and laws cannot form the basis of a charge/indictment in foreign countries.

*****

At this juncture, it should be noted that geolocation technology is not sufficient for solving the jurisdictional question.[41] It is may be acceptable for business, but not suitable for the jurisdictional question, which involve sovereignty and the protection of a States' citizens.

Geolocation allows, for example, a newspaper to locate customers invisibly from the receiver's perspective. Essentially, the more precisely the software gives a location, the more unavoidable is the intrusion/violation of privacy.

Furthermore, geo-location tracking software[42] often bases its determination on the IP address, but there is no inherent connection between an IP address and its physical location.[43] A geolocation

---

[40] On the "effect test", see SPANG-HANSSEN-2 *supra* note 3, at 247-249 & 348-365 referring to several cases in the footnotes.

[41] SPANG-HANSSEN-3 *supra* note 8, at 218-221.

[42] Many names or terms have been given to this software, for example GeoIP, IP-location, Geo-computing, and User-location. See also Teemu Ross et al., *A Probabilistic Approach to WLAN User Location Estimation*, INTERNATIONAL JOURNAL OF WIRELESS INFORMATION NETWORKS, p. 155, Vol. 9, no. 3, July 2002, also at www.cs.helsinki.fi/u/ttonteri/pub/ijwin02.pdf (visited March 2006).

[43] SPANG-HANSSEN-2 *supra* note 3, at 333-339. Otherwise, Dan Svantesson, *Geo-Location Technologies and other Means of Placing Borders on the "Borderless" Internet*, 23 J. MARSHALL J. COMPUTER & INFO. L. 101, 111 (Fall 2004), who thinks present geo-location software is sufficiently accurate for legal purposes, even though he points out that "the accuracy of these products is difficult to gauge." However, for example, ECommerce Taxation and the Limitations of Geolocation Tools pages 3-5 & 7, Information Technology Association of America (ITAA) acknowledge that geolocation software only can check the geographic location of the point where the user's computer signal enters the Internet (i.e., the customer "joins the Internet"), but not the location of the user and only within 50 miles under the very best of circumstances. The examination paper notices that larger IP-address-users under IPv4 may only have a single bloc of IP addresses for the whole world. It further points out that delays in reflecting changes in reassignments or incorrect changes to router tables will negatively impact the overall quality of the correctness of a geographic location. Another problem is that if a customer is not accessing a POP from the same geographic area as the POP server itself – which the geolocation technologies assume – then the geolocation soft-are will send back inaccurate customer location data. For this reason wireless Internet access presents unique problems. If a customer chooses to connect into an ISP outside of his/her local telephone calling area, his/her location will not be correctly reported by the geolocation software -- for example, where a user calls an ISP via a POP call-in number located in another state or country. In addition, the future IPv6 protocol, which will have far more IP addresses and thus imply far more (dynamic) reassignment of IP addresses, will probably overwhelm geolocation software capacities, at www.itaa.org/taxfinance/docs/geolocationpaper.pdf (visited March 2006).

system uses algorithms to check the location of the potential buyer or, more correctly, his/her computer's IP address. However, there is no reliable, foolproof method.[44]

In contrast, technology to resolve the jurisdictional question in cybercrime must be 100% reliable and unbreakable.

3.3.4. Enforcement

Because, for Cyberspace cases, it is more than likely that a cross-border situation will be involved, enforcement jurisdiction has become essential for States to live up to their legislation.[45] What does it matter that each State makes jurisdictional rules with exterritorial reach if it cannot enforce its decisions and its courts' judgments?

Enforcement jurisdiction might, to a degree not seen before, limit a State's legislative wishes, as one or more foreign States might not allow enforcement of the first State's cross-border legislation. As a matter of international law, no State is generally entitled to require the commission of a criminal offence or an illegality within the territory of another State.[46]

For Cyberspace, it might be that Professor F.A. Mann's well-known statement on recognition has even more weight, namely, that: "it may be international law cares, not about legislative jurisdiction, but only about enforcement[47] jurisdiction."[48]

This statement seems certainly to have turned out to be true after the invention of the Internet – and the accompanying attempts of different states to legislate and of their courts to issue decisions about the international effects of Internet use. But actual enforcement of a State's legislation and court decisions has been minimal, as foreign states where the alleged defendant have been resident have not been willing to extradite. Thus, the citizens of the State seeking to legislate/adjudicate have been left with an unenforceable, in fact, worthless, decisions (as in the case of SUE above).

Thus, if the formulation of jurisdictional rules is not the first choice of the international community, then maybe it should instead create at least an initial framework on how enforcement of a State's court decisions over Cyberspace acts might be accomplished.

4. A Road Map

There must be new rules of public international law governing cyberspace and the limits of national jurisdiction over Cyberspace, including that:

- What a cybernaut does on the Internet is most likely an international case – thus, not subject to domestic law alone, and that a domestic court must consider international and foreign law.
- Public international law must resolve the question of where "the place" of the criminal act is.[49]
- Let it be stated by the international society that what is done legally in the cybernaut's own country shall not cause such individual to be charged or indicted in a foreign country or countries – except for cases of extreme harm that are reasonably foreseeable.

---

[44] SPANG-HANSSEN-3 *supra* note 8, at 218-221. Certain methods of "detective work" can be found in, for example, Uri Raz, *How do I find the geographical location of a host, given its IP address?*, at www. private.org.il/IP2geo.html (visited June 2003).

[45] SPANG-HANSSEN-2 *supra* note 3, at 365-366. Para. 8 in Explanatory Memorandum to the Cyberspace Convention: "By connecting to communication and information services users create a kind of common space, called "cyber-space", which is used for legitimate purposes but may also be the subject of misuse. These "cyber-space offences" are either committed against the integrity, availability, and confidentiality of computer systems and telecommunication networks or they consist of the use of such networks of their services to commit traditional offences. The transborder character of such offences, e.g. when committed through the Internet, is in conflict with the territoriality of national law enforcement authorities." See http://conventions.coe.int/ treaty/EN/cadreprojects.htm (visited June 2001).

[46] F.A. MANN, FURTHER STUDIES IN INTERNATIONAL LAW 31 (1990, Clarendon Press, Oxford).

[47] SPANG-HANSSEN-2 *supra* note 3, at 437-441.

[48] F.A. MANN, FURTHER STUDIES IN INTERNATIONAL LAW 18 (1990, Clarendon Press, Oxford).

[49] A separate paper of mine will deal with this vital issue for Cyberspace.

Next, the international community must decide on the rest of the Standards and Norms for Cyberspace issues. For example, to what extent – if any – should "spamming" be considered a (cyber-)crime?[50] The percentage of electronic spam often appears similar to the percentage of unsolicited mail in a physical mailbox. Thus, spam could be held to be a "service-provider problem" (that is, not having enough copper wire/broadband for PR-commercials) rather than regarded as a crime similar to a distribution of service attack ("DoS") (that is, making a computer resource unavailable to its intended users by intentionally overwhelming it with data – "a network terrorist attack").

As for acts that are not destructive of computer networks – that is, pure information on the Internet – a lesson could be learned from developers of the Internet Protocol, who stated: "Be liberal in what you accept, and conservative in what you send" and who also suggested that we "teach our children to think more deeply about what they see and hear" because "[t]hat, more than any electronic filter [and laws], will build a foundation upon which truth can stand."

Then – and only then – will it be possible to decide what should be a cybercrime and how to prevent it – through education of computer users and others associated with the Internet.

*****

Maybe the time has come – as far as for "pure online" incidents – in which Nations should give up making it possible for plaintiffs to go on forum shopping "sprees" and to return instead to the old basic rule, that is, that if a person wishes to sue someone else for a computer-related act, he/she must go to the defendant's forum. After all, airplanes make it easy and economically possible for a plaintiff to go to the defendant's forum. One can only hope also that the single consumer, who in practice often has no problem using the most advanced computer game, will be forced to learn that by logging in to the Internet he/she has removed him/herself from the local community's consumer protection and as a tourist has gone to a foreign nation. That nation will most likely have different rules and laws that have to be read and studied, instead of carelessly ignored or disregarded by "surfing" websites and clicking links without reading user conditions, etc.

Today, for that matter, all online customers are also tourists who travel to faraway places with totally different laws from that of their home forums. Thus, these customers are – at least in certain weeks of the year - used to being under and subject to foreign legal rules – why not also let this be the case for pure online cross-border disputes!?![51]

5. Final Remarks

The public international computer network can only work if States do not make it into chaos. Their citizens want to use it, and they want speed for their voice-IP, video and game, as well as stability/predictability. They prefer global reach and no censorship, rather than having the net slowed down because of national filters. And they do not want the risk of incurring Global Jurisdiction, which also indirectly advances pernicious world-wide forum shopping by plaintiffs.

As indicated above, a State is not allowed to exercise Global Jurisdiction[52] – distinguished from Universal Jurisdiction - under public international law, which requires sufficient closeness (a close link) and reasonableness. This also implies that a narrow community view[53] will only be acceptable under public international law as long as a statute or court decision does not reach outside the national border of the forum State.

Legislators must find other ways to legislate than software coding on devices on the public international computer networks. They can choose to legislate on the hardware (nodes) inside their

---

[50] Cybercrime offences under national law usually deal with: A. Have illegal access to computer data and systems, illegal interception, data interference, and system interference been criminalized? B. Have computer-related forgery and fraud been criminalized? C. Have the necessary substantive and procedural laws to prevent and punish terrorist and other criminal activities perpetrated with the aid of computers and computer networks been enacted? Section 3.1.9, page 7 in CRIMINAL JUSTICE ASSESSMENT TOOLKIT: CROSS-CUTTING ISSUES # 4 - INTERNATIONAL COOPERATION (UNODC, 2006) at http://www.unodc.org/documents/justice-and-prison-reform/cjat_eng/4_International_Cooperation.pdf (last visited 10 March 2010).

[51] SPANG-HANSSEN-2 *supra* note 3, at 172-173.

[52] Compare the definition above at footnote 12.

[53] For example, see the discussion by the U.S. Supreme Court in *Reno v. American Civil Liberties Union*, 521 U.S. 844, 877 (US, 1977).

own country, but this – as stated above – prevent "full membership" in the public international computer network and preclude valuable computer "pipelines".

The international community really must quickly decide what are the (very) serious computer-related crimes and what crimes allow exercise of Universal Jurisdiction; but it should not accept States' national-law attempts at exercising Global Jurisdiction.

The world is based on States and their constitutions/laws set the limits for what their citizens legally can and cannot do, as well as to what extent they can expect their governments to protect them.

Once more, we need a truly international Internet Crime Convention that prevents Internet users from being indicted in foreign countries for criminal violations of which they cannot reasonably be held to be aware.

I sincerely hope this Congress will consider asking the UN Commission on Crime and Criminal Justice to draft and prepare for the next Congress an Internet Crime Convention related to crimes where a computer has been used, which:

- integrates UN Crime Prevention and Criminal Justice Standards and Norms
- suggests how best to provide international education and training on the use of Cyberspace – without risk of charge/indictment anywhere on the planet.
- deals with protection[54] of the individual cybernaut from criminalization of his/her acts by foreign states and resulting extradition – except in cases where the international community has expressly condemned particular (universal) acts.

But first of all, the international community must decide whether it wants one jurisdiction for cyberspace or whether it wants to keep true to the traditional principle of equal sovereignty of all States on the planet. And for the latter, each State must declare it agrees with the principle that: "what is done legally in the cybernaut's own country shall not cause such individual to be charged or indicted in a foreign country or countries – except for cases with extreme destructive effects that are reasonably foreseeable."

[54] Incorporating, but not limited to, the scope of: African Charter on Human and Peoples' Rights 1986; African Charter on the Rights and Welfare of the Child 1990; Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms 1953; American Convention on Human Rights 1969; (OAS) American Declaration of the Rights and Duties of Man, O.A.S. Res. XXX [AG/RES. 1591 (XXVIII-O/98)], adopted by the Ninth International Conference of American States, Bogotá, Colombia (1948); European Convention for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment 1989. Annex A, page 31 in CRIMINAL JUSTICE ASSESSMENT TOOLKIT: CROSS-CUTTING ISSUES # 2 - JUVENILE JUSTICE (UNODC, 2006) at http://www.unodc.org/documents/justice-and-prison-reform/cjat_eng/2_Juvenile_Justice.pdf (last visited 10 March 2010).

APPENDIX 1: Article 22 of CyberCrime Convention of 2001[55] (Jurisdiction)

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a. in its territory; or
b. on board a ship flying the flag of that Party; or
c. on board an aircraft registered under the laws of that Party; or
d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

[55] See http://conventions.coe.int/treaty/en/treaties/html/185.htm (last visited 9 March 2010).