Cybercrime, Cyberterrorism and Jurisdiction: An Analysis of Article 22 of the COE Convention on Cybercrime

Armando A. Cottim[א]

Introduction

Ever since Cain and Abel, crime is a "known known" to human kind. Modern criminal codes have dealt quite well with crime within territorial boundaries and even, sometimes, outside those boundaries, by applying themselves to crimes committed by nationals abroad. Criminal law has then been almost purely domestic, with external threats to the public order of States being dealt with by the military.

Yet, the revolution in information technologies has changed society to a point where advances in programming artificial intelligence software and in the processing capacity of desktop and/or laptop computers are leading society to a time when a cyberbot will be impossible (or at least very difficult) to distinguish from a human person.[1]

And the advent of cyberspace has changed the established criminal law model. Online crime happens without boundaries, as attacks can come from outside the borders of one State, thus scattering crime scenes through two or more countries, sometimes in more than one continent.[2]

Solutions to the problems posed must be addressed by international law, through the adoption of adequate international legal instruments.[3] The Convention on Cybercrime, opened

---

[א] The author has a 5-year law degree achieved at the Lisbon University, Lisbon, Portugal, and was awarded a Master's degree in International Law, by the same University, with a dissertation on Terrorism at Sea in International Law. Being a scuba diving instructor, a musician, a computer programmer and a certified network engineer, his interests float between music, sea and cyberspace. Comments are welcome and can be sent to his email address (armando@cottim.net).

[1] Thus, **JOHN J. STANTON**, "Terror in Cyberspace. Terrorists Will Exploit and Widen the Gap between Governing Structures and the Public", in *American Behavioral Scientist*, vol. 45 (2000) p. 1022.

[2] Conveying a similar idea, **SUSAN W. BRENNER** and **JOSEPH J. SCHWERHA IV**, "Cybercrime Havens: Challenges and Solutions", *Business Law Today*, vol. 17 (November/December, 2007), p. 49.

[3] For a thorough study of the relationship between international conventions and international customary law, with special interest in *ius cogens* rules, see **EDUARDO CORREIA BAPTISTA**, *Ius Cogens em Direito Internacional*, Lisboa, Lex, 1977, pp. 491 *et passim*.

for signature in Budapest, November 23, 2001 and entered into force in 2004,[4] aimed to meet this challenge – respecting human rights – in the new reality we now call Information Society.

However, although jurisdiction issues were addressed by the Convention on Cybercrime, some weaknesses prevent this Convention from being more effective in making international cooperation the solution for cybercrime. As an additional problem, cyberterrorism also became a hazard the international community has to deal with.

Even if it seems to be a real threat,[5] cyberterrorism is a scare word that plays with the fear of two generally known unknowns – terrorism and technology[6] – and discussions rage the international *fora* dealing with terrorism, crime and cybercrime as to the reality of this threat.

Our initial concern will therefore be the analysis of article 22 of the Convention on Cybercrime, first discussing general jurisdiction theories and then the theories applied by the Convention, together with other issues dealt with in the article. Then, a discussion of several cases dealing with jurisdiction, international cooperation and cybercrime will take us to some reflection on cyberterrorism and the applicability of the jurisdiction rules of the Convention on Cybercrime in cyberterrorism cases.

I. Article 22. The Analysis

A. Jurisdiction theories

No less than five different jurisdiction theories have been applied altogether by courts and governments, all leading to the ascribing of jurisdiction to one court and adversely affecting other courts' jurisdiction.

1. Territoriality theory

---

4 In accordance with article 36, paragraph 3 of the Convention on Cybercrime, after Albania (signed: November 23, 2001, ratified: June 20, 2002), Croatia (signed: November 23, 2001, ratified: October 17, 2002), Estonia (signed: November 23,/2001, ratified: May 12, 2003), Hungary (signed: November 23,/2001, ratified: December 4, 2003), and Lithuania (signed: 23/6/2003, ratified: March 18, 2004), all members of the Council of Europe, have expressed their consent to be bound by the Convention. For a list of the States that signed and ratified the Convention, see "Convention on Cybercrime. CETS No.: 185", online at http://conventions.coe.int.

5 For an examination of the use of the Internet by terrorists, extremists and activists, see **KATHY CRILLEY**, "Information warfare: new battlefields, Terrorists, propaganda and the Internet?" in Alan O'Day (ed.), *Cyberterrorism*, Aldershot, Ashgate Publishing Limited, 2004, pp. 67-74. For a discussion of the widespread use of information technology by terrorist-type organizations in recent years, for propaganda, fundraising, information dissemination and secure communications, see **S. M. FURNELL** and **M. J. WARREN**, "Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium?" in Alan O'Day (ed.), *Cyberterrorism*, pp. 113-115.

6 See **AYN EMBAR-SEDDON**, "Cyberterrorism: Are We Under Siege?" in Alan O'Day (ed.), *Cyberterrorism*, p. 11.

The theory that jurisdiction is determined by the place where the offence is committed, in whole or in part ("territoriality theory"), derives from the Westphalian[7] model of sovereignty, which is said to include three fundamental principles: ① exclusive control over the nation's territory, ② non-interference, and ③ equality between States.[8] Although discussed and opposed,[9] the model seems to have, at least, a general acceptance in what concerns theses principles, even if the equality between the States is most of the times only formal.[10]

Given that the State has sovereignty over the territory, it will obviously have jurisdiction over any misconduct which occurs in that territory,[11] whether perpetrated or not by one of its nationals.[12]

A complex case of application of the territoriality theory is *Bavaria v. Somm*, tried at the *Amtsgericht* of Munich, Germany, in 1999. As Managing Director of CompuServe

---

[7] On the Westphalia treaties, see **CHRISTOPHER HARDING** e **C. L. LIM**, "The Significance of Westphalia: An Archaeology of the International Legal Order", *in* Christopher Harding and C. L. Lim (eds), *Renegotiating Westphalia: Essays and Commentary on the European and Conceptual Foundations of Modern International Law*, The Hague / Boston / London, Martinus Nijhoff Publishers, 1999, pp. 1-23.

For a vision on the centrality of the concept of sovereignty derived from Westphalia and the various international relations theories (Marxism excepted), see **STEPHEN D. KRASNER**, *Sovereignty: Organized Hypocrisy*, New Jersey, Princeton University Press, 1999, pp. 44-46.

[8] Thus, **JOAN FITZPATRICK**, "Sovereignty, Territoriality, and the Rule of Law", *Hastings International and Comparative Law Review*, vol. 25 (2002), pp. 304,310. **SEYOM BROWN**, *International Relations in a Changing Global System: Toward a Theory of the World Polity*, Boulder, Colorado, Westview Press, 1992, p. 74, however, refers only two principles: one according to which a State is "unequivocally sovereign within its territorial jurisdiction", and the principle of non-interference.

[9] **CHRISTOPHER C. JOYNER** and **WAYNE P. ROTHBAUM**, "Libya and the Aerial Incident at Lockerbie: What Lessons for International Extradition Law?", *Michigan Journal of International Law*, vol. 14 (Winter, 1993), pp. 256, 257, refer that "the Westphalian concept of absolute State sovereignty is undergoing challenge from the community conception espoused by the U.N. Charter", and **STÉPHANE BEAULAC**, *The Power of Language in the Making of International Law: The Word Sovereignty in Bodin and Vattel and the Myth of Westphalia*, Leiden / Boston, Martinus Nijhoff Publishers, 2004, pp. 71 *et passim*, considers the Westphalian system as a myth, given the centralizing relevance of the sovereignty concept in Bodin and the externalization of authority that Vattel sees in the concept.

[10] Thus, **FRANCISCO FERREIRA DE ALMEIDA**, *Direito Internacional Público*, 2ª ed., Coimbra, Coimbra Editora, 2003, p. 15.

[11] Thus, **FRANCESCO ANTOLISEI**, *Manuale di Diritto Penale. Parte Generale*, 15ª ed., Milano, Dott. A. Giuffrè Editore, 2000, p. 118.

[12] A comparative study of several penal codes in Europe shows that all consecrate the principle of territoriality. Thus, article 6 of the Italian *Codice Penal* states that "Chiunque commette un reato nel territorio dello Stato è punito secondo la legge italiana." Following the same path, article 113-2 of the French *Code Pénal* states: "La loi pénale française est applicable aux infractions commises sur le territoire de la République", section 3 of the German *Strafgesetzbuch* states "[d]as deutsche Strafrecht gilt für Taten, die im Inland begangen werden" and article 4 of the Portuguese *Código Penal* states that "[s]alvo tratado ou convenção internacional em contrário, a lei penal portuguesa é aplicável a factos praticados em território português, seja qual for a nacionalidade do agente."

Information Services GmbH, Felix Bruno Somm, a citizen from Switzerland, was charged in Germany with being responsible for the access – in Germany – to violent, child, and animal pornographic representations stored on the CompuServe's server placed in the USA.[13] The court considered it had jurisdiction over Mr. Somm because, even though he was Swiss, he lived in Germany.[14]

2. Nationality theory

The "nationality theory" is also called "active personality theory" because it deals primarily with the nationality of the person who committed the offence.[15] Being widely recognised that a country has almost unlimited control over its nationals,[16] said country is considered to have the right to exercise jurisdiction over those individuals, wherever they are and whatever they do.[17] Wherever the offence is committed – at home or abroad – the offender probably has better knowledge of the laws of his own State than of the laws of the other State. Also, an act can be considered legal in the territory where it was committed, whereas it can be considered a crime in the person's homeland.[18]

The case *United States v. Galaxy Sports* seems to be a good example[19] of the application of this theory.[20] World Sports Exchange, together with its President Jay Cohen,

---

13 *People v. Somm*, Case 8340 Ds 465 Js 173158/95 (Amtsgericht, München, Bavaria, 1999). See, also, **THOMAS STADLER**, *Der Fall Somm (CompuServe)*, online in http://www.afs-rechtsanwaelte.de/urteile/artikel06-somm-compuserve1.php, last visited September 2, 2008.

14 Mr. Somm was sentenced to an overall term of imprisonment of 2 years (paragraph II of the sentence), even if the following paragraph of the sentence suspended (*ausgesetzt*) it's execution on probation.

15 Thus, **CHRISTOPHER L. BLAKESLEY**, "Jurisdictional Issues and Conflicts of Jurisdiction", *in* M. Cherif Bassiouni (ed.), *Legal Responses to International Terrorism. U.S. Procedural Aspects*, Dordrecht, Martinus Nijhoff Publishers, 1988, p. 139.

16 Thus, **RAY AUGUST**, "International Cyber-Jurisdiction: A Comparative Analysis", *American Business Law Journal*, vol. 39 (Summer, 2002), p. 539.

17 This statement is not supposed to be understood in an active, dictatorial sense (where the State controls every aspect of the citizens' life), but in a passive, securitarian sense (where the State has the responsibility to protect society against criminal behaviour).

18 The European penal codes mentioned above considerer themselves as having jurisdiction with regard to certain actions committed abroad by nationals. Thus, article 9 of the Italian *Codice Penale*, article 113-6 of the French *Code Pénal*, section 5 of the German *Strafgesetzbuch* and article 5 of the Portuguese *Código Penal*.

19 The sentencing of Robert Matthew Bentley, a citizen of the USA, to 41 months in prison, followed by three years supervised release, together with a restitution of $65,000, by the federal grand jury in Pensacola, Florida, USA, presided by United States District Judge Richard Smoak, in November 2007, for crimes committed in Europe through the Internet, seems to be another good example of application of the nationality theory for jurisdiction assumption. See **UNITED STATES ATTORNEY'S OFFICE, NORTHERN DISTRICT OF FLORIDA**, "International Computer 'Hacker' Sentenced to More Than Three Years in Federal Prison", online at http://www.usdoj.gov/criminal/cybercrime/bentleySent.pdf, last visited September 2, 2008.

was one of the defendants. The company targeted customers in the United States, advertising its business all over America by radio, newspaper, and television. Its advertisements invited clientele to bet with the company either by toll-free telephone or through the Internet. [21] Because the company was Antigua-based, the court was unable to assert jurisdiction over it. It's President, however, was a citizen of the USA and could, therefore, be taken to court. Mr. Cohen was – on August 10, 2000, after a jury trial presided by Judge Thomas P. Griesa – sentenced to a term of twenty-one months' imprisonment.[22] Dealing with the appeal to this sentence, the Second Circuit Court of Appeals affirmed the judgment of the district court without even discussing the assumption of jurisdiction.[23]

3. Passive personality theory

While the "nationality theory" deals with the nationality of the offender, assigning jurisdiction to his/her homeland courts, its opposite – the "passive personality theory" – is concerned with the nationality of the victim. [24] The reasons for ascertaining jurisdiction over an offence are similar for both – the almost unlimited control over a country's nationals – but are now seen from the opposite point of view. Thus, when we follow this theory, the courts of the State to which the victim belongs assume jurisdiction. [25,26]

---

[20] This case was the first U.S. federal action against operators of offshore companies using Web sites to facilitate illegal gambling. The complaint names six companies, one of which is Antigua-based World Sports Exchange. For a short description of the case, see *United States v. Galaxy Sports*, Digestible Law. Perkins Coie's Internet Case Digest, online at http://www.digestiblelaw.com/gambling/blogQ.aspx?entry=2305&id=16, last visited September 2, 2008.

[21] For a short description of the company's activity, see *USA v. Cohen*, Second Circuit Court of Appeals, online at http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=2nd&navby=docket&no=001574, last visited September 2, 2008.

[22] Of which he seems to have served 17 months. See **BENNET KELLEY**, "Crystalball.Gov: Predicting Cyber Policy in 2008", *Journal of Internet Law*, vol. 11 (March, 2008), p. 21.

[23] See *USA v. Cohen*, Second Circuit Court of Appeals, online, quoted. For a short description of the consequences derived from Mr. Cohen's conviction, see **KATHRYN B. CODD**, "Betting On The Wrong Horse: The Detrimental Effect of Noncompliance in the Internet Gambling Dispute on the General Agreement on Trade in Services (GATS)", *William and Mary Law Review*, vol. 49 (December, 2007), pp. 946 *et passim*.

[24] Thus, **CHRISTOPHER L. BLAKESLEY**, "Jurisdictional Issues and Conflicts of Jurisdiction", p. 139.

[25] Thus, **JOAN FITZPATRICK**, "Sovereignty, Territoriality, and the Rule of Law", *Hastings International and Comparative Law Review*, vol. 25 (2002), p. 313, note 37.

[26] Article 10 of the Italian *Codice Penale*, article 113-7 of the French *Code Pénal*, Section 7 of the German *Strafgesetzbuch* and article 5 of the Portuguese *Código Penal* apply the respective national criminal law to acts against the nationals of these countries.

Good examples of this assumption are the interception of the Egyptian plane that carried the *Achille Lauro* perpetrators by USA planes,[27] and the dispute between the USA and Italy regarding their judgment,[28] together with the several cases presented by the family of Mr. Leon Klinghoffer in North American courts against the Palestinian Liberation Organization, the Lauro company, ABC Tours, Chandris, Inc. (the company that chartered the boat) and the Port of Genoa, Italy.[29]

In the field of cybercriminology, a fine example of jurisdiction assumption by application of the passive personality theory is the sentencing, on July 25, 2003, at the federal courthouse in Hartford, Connecticut, USA, by United States District Judge Alvin W. Thompson, of the Russian citizen Alexey Ivanov, who lived in Chelyabinsk, Russia, for hacking into computers in the United States.[30,31]

4. Protective theory

The "protective theory" (also called "security principle" and "injured forum theory") is probably the least used – if ever – of the theories that sanction jurisdiction. Dealing with the national or international interest injured, this theory permits the assignment of jurisdiction to the State that sees its interest – whether national or international – in jeopardy because of an offensive action.[32] In any case, there seems to be a general trend for penal laws to include this

---

27 For a careful description of the facts, see **ANTONIO CASSESE**, *Terrorism, Politics and Law: The Achille Lauro Affair*, Cambridge, Polity Press, 1989, pp. 31-43.

28 For all matters dealing with the interception and subsequent reactions, see **GREGORY V. GOODING**, "Fighting Terrorism in the 1980's: The Interception of the Achille Lauro Hijackers", *Yale Journal of International Law*, vol. 12 (1987), pp. 158-161.

29 For a description of the civil suits arising out of the *Achille Lauro* incident, see **DEAN C. ALEXANDER**, "Maritime Terrorism And Legal Responses", *Transportation Law Journal*, vol. 82 (1991), pp. *467 et passim*.

30 *U.S.A. v. Ivanov* (2003), 172 C.C.C. (3d) 551 (Nfld.C.A.). See also **U.S. DEPARTMENT OF JUSTICE. UNITED STATES ATTORNEY**, "Russian Man Sentenced for Hacking into Computers in the United States", online at http://www.usdoj.gov/criminal/cybercrime/ivanovSent.htm, last visited September 2, 2008.

31 Another example is the sentencing – in the federal court of Manhattan, Southern District of New York – of the Kazakhstan citizen Oleg Zezev to 51 months in prison, for extortion and computer hacking charges, due to facts that occurred while he was still living in Almaty, Kazakhstan. See **U.S. DEPARTMENT OF JUSTICE. UNITED STATES ATTORNEY**, "Kazakhstan Hacker Sentenced to Four Years Prison for Breaking into Bloomberg Systems and Attempting Extortion", http://www.usdoj.gov/criminal/cybercrime/zezevSent.htm, last visited September 2, 2008.

32 Thus, **CHRISTOPHER L. BLAKESLEY**, "Jurisdictional Issues and Conflicts of Jurisdiction", p. 139.

theory,[33] sometimes restricting the application to certain crimes, like counterfeiting of money and securities.

5. Universality theory

Finally, the "universality theory" is based on the international character of the offence and, contrary to the other theories, allows every State the claim of jurisdiction over offences, even if those offences have no direct effect on the asserting State, [34] therefore demanding no nexus between the State assuming jurisdiction and the offence itself.

Two requirements are necessary for assuming jurisdiction: ① the State assuming jurisdiction must have the defendant in custody,[35] and ② the crime must be especially offensive to the international community.[36] Thus, the first crime to be considered for universal jurisdiction was piracy, followed by slave traffic.[37]

After WW II, war crimes, crimes against humanity, certain terrorist acts, hijacking and sabotage of planes, apartheid, torture and other violations of human rights progressively became subject to universal jurisdiction.[38]

---

33 See *Codice Penale* article 7, *Code Pénal* article 113-10, *Strafgesetzbuch* section 6, and *Código Penal* article 5, number 1, *littera* a) (which specifically deals, *inter alia*, with computer crime).

34 Thus, **CHRISTOPHER L. BLAKESLEY**, "Jurisdictional Issues and Conflicts of Jurisdiction", p. 141.

35 Questionable means (like abduction) may sometimes have been employed for this. The assumption of jurisdiction over what was (wrongly) considered as piracy led to a questionable action of the USA navy fighters over the commercial plane taking the *Achille Lauro* terrorists from Egypt, after the release of the ship. The Egyptian plane was diverted to a NATO base in Italy. What having the defendant in custody often requires is international cooperation. So, **M. CHERIF BASSIOUNI**, "Policy Considerations on Inter-State Cooperation in Criminal Matters", *Pace Yearbook of International Law*, vol. 4 (1992), pp. 126-128. Thus, *v.g.* in the case of Oleg Zezev, Mr. Zezev was called for a meeting in the U.K. and the British police seized him after he recognized the facts of his crime in the presence of a disguised British police officer.

36 Thus, **M. CHERIF BASSIOUNI**, *Crimes against Humanity in International Criminal Law*, Dordrecht, Martinus Nijhoff Publishers, 1992, pp. 511-513. Mr. Bassiouni also refers that, in the Middle Ages, some cities in Northern Italy would seize and/or persecute certain types of criminals (those they called *banditi*, *vagabundi* and *assassin*) when they were under their jurisdiction, even if the crime was committed elsewhere, therefore applying the principle of universal jurisdiction for specific crime types. **M. CHERIF BASSIOUNI**, *Crimes against Humanity in International Criminal Law*, p. 513.

37 Thus, *inter alia*, **KENNETH C. RANDALL**, "Universal Jurisdiction under International Law", *Texas Law Review*, vol. 66 (March, 1988), p. 788.

38 Thus, **ERIC S. KOBRICK**, "The Ex Post Facto Prohibition and the Exercise of Universal Jurisdiction over International Crimes", *Columbia Law Review*, vol. 87 (November, 1987), pp. 1523, 1524. This idea is shared by **THOMAS H. SPONSLER**, "The Universality Principle of Jurisdiction and the Threatened Trials of American Airmen", *Loyola Law Review*, vol. 15 (1969), p. 49, who mentions the Nuremberg and Tokyo trials, after the end of WW II, as the concept's expansion moment.

JAMES D. FRY, "Terrorism as a Crime against Humanity and Genocide: The Backdoor to Universal Jurisdiction", *UCLA Journal of International Law and Foreign Affairs*, vol. 7 (2002), p. 176, refers that the UN

B. Jurisdiction Theories applied by the Convention

An analysis of the several *litterae* of paragraph 1 of article 22 of the 2001 Budapest Convention on Cybercrime (hereafter "the Convention") shows that the Convention relies exclusively on the territoriality and nationality theories to empower parties to establish jurisdiction.

According to *litterae a* to *c*, any offence established under articles 2 through 11 of the Convention that has occurred in the territory of one Party, in a ship flying its flag or in an aircraft registered under its laws, is to be prosecuted in that State.[39] A Party is, therefore, asked by the Convention to assert territorial jurisdiction if both the person attacking a computer system and the attacked system are located within its territory. The same would be true when the attacked computer system is within a Party's territory, even if the attacker is in another country.

Litterae b and *c* specifically require each Party to establish criminal jurisdiction over offences committed on board of ships flying its flag or aircraft registered under its laws. Already implemented in the laws of many States,[40] this type of jurisdiction assumption is

---

General Assembly codified the universality principle, applied in Nuremberg, to war crimes, crimes against humanity and aggression crimes.

The Geneva Conventions of 1949 codified the universality principle in relation to war crimes. The 1948 Genocide Convention did not apply universal jurisdiction to genocide because France, the Soviet Union and the USA opposed, but many courts applied the principle to genocide, considering this should be considered customary international law. Thus, **KENNETH C. RANDALL**, "Universal Jurisdiction under International Law", p. 789.

On the other hand, **JONATHAN I. CHARNEY**, "Progress In International Criminal Law?", *American Journal of International Law*, vol. 93 (April, 1999), p. 454, considers that the international illegality of acts such as genocide, crimes against humanity, war crimes and similar will be reinforced as a result of the statute of the International Criminal Court, showing these acts were seen as international crime before that moment.

According to **JAMES D. FRY**, "Terrorism as a Crime against Humanity and Genocide", p. 176, the principle of universality has been expanded, since de 1940s, to include torture, slave traffic and drug traffic.

[39] The fact that a Council of Europe-sponsored Convention follows this path is not surprising, given that, traditionally, the European Court of Human Rights defends an essentially territorial notion of jurisdiction. Thus, *inter alia*, *Öcalan v. Turkey* (Application no. 46221/99), Judgment, 12 March 2003, paragraph 93, and the decision of inadmissibility of *Banković and Others v. 17 countries* (Vlastimir and Borka Banković, Živana Stojanović, Mirjana Stoimenovski, Dragana Joksimović and Dragan Suković against Belgium, the Czech Republic, Denmark, France, Germany, Greece, Hungary, Iceland, Italy, Luxembourg, the Netherlands, Norway, Poland, Portugal, Spain, Turkey and the United Kingdom), Application no. 52207/99, paragraphs 59-61.

[40] Ships are frequently considered to be an extension of the territory of the State. The same applies, *mutatis mutandi*, to aircrafts.

Based on article 91 of the UN Convention on the Law of the Sea, the applicability of the territorial principle to ships should be transparent. Because this was already expressed in 1927, in *The Case of the S.S. "Lotus"*, where the Permanent Court of International Justice assimilated a ship (the Turkish *Boz-Kourt*) to the territory of its Flag state, it would seem to be a very well established principle. Nevertheless, it wasn't so! In fact, just one year after the *Lotus* decision we find decisions in the opposite direction, held by North American courts,

most useful where the ship or aircraft is not located in the Party's territory (or territorial waters/pace) at the time of the commission of the crime.

Then, according to *littera d*, when one national of one State Party commits one of the Convention-laid down offences in another State, the State of nationality of the offender also has to establish jurisdiction provided, however, the target State criminalises the said offence[41] or the offence was committed outside territorial jurisdiction, of any State, *v.g.* in the High Seas.[42]

Paragraph 4 of the Convention further allows Parties to establish jurisdiction in conformity with their domestic law, which enlarges the base for jurisdiction should a State Party so desire.[43]

C. Non-application clause

Paragraph 2 of article 22 of the Convention allows Parties to reserve the right to apply – or not – the jurisdiction grounds established in *litterae b* to *d*. States are thus given a great deal of liberty regarding issues related with cybercrime, even if they cannot avoid the obligation of prosecution when the offence is committed in their own territory (paragraph 1, *littera* a).

In practice, and since some offences affect several countries at the same time, this non-application clause could result in no country claiming jurisdiction over one given offence, thinking that surely other countries will have suffered more damage and will, therefore, have priority in prosecuting.[44] Therefore, this paragraph should also include an obligation for affected Parties to consult with each other, so no offence is left without appropriate punishment.

---

v.g. in *Lam Mow v. Nagle*, 24 F.2d 316 (9th Cir., 1928) and *Wong Ock Jee v. Weedin*, 24 F.2d 962 (9th Circ. 1928).

41 Which means the target State might not be Party to the Convention.

42 In this case, it is our understanding that the target of the offence could also be outside territorial jurisdiction.

43 As an example of this enlargement of jurisdiction, the *Strafgesetzbuch* applies itself to certain acts (*v.g.* assaults against air and sea traffic – *Angriffe auf den Luft- und Seeverkehr* – or trafficking of human beings for sexual exploitation – *Menschenhandel zum Zweck der sexuellen Ausbeutung*) committed abroad regardless of the law of the place of their commission (*unabhängig vom Recht des Tatorts*). See *Strafgesetzbuch*, Section 6.

44 See **SUSAN W. BRENNER** and **BERT-JAAP KOOPS**, "Approaches to Cybercrime Jurisdiction", *Journal of High Technology Law*, vol. 4 (2004), p. 3. The authors mention the fictitious example of a "script kiddie" who "concocts a new worm and, without really thinking of the potential consequences, launches it on the Internet", "causing significant damage in numerous countries around the world."

Also, to our understanding, this paragraph seems to be in absolute contradiction with the wording of paragraph 1, which transmits the idea that the adoption, by Parties, of legislative (and other) measures to establish jurisdiction is injunctive.

D. *Aut dedere aut judicare*

Paragraph 3 of article 24 establishes the international customary law[45] principle *aut dedere aut judicare*.[46] Should ① the alleged offender be found in the territory of one Party State (different from the one where the offence was committed), ② an extradition be required by the offended State, and ③ the Party in which territory the alleged offender (requested Party) is constrained by domestic law not to extradite,[47] the requested Party has the duty to prosecute, as well as the legal ability to undertake investigations and proceedings domestically.[48] The underlying idea is the need to ensure that no offence goes unpunished.

The fact that the obligation to prosecute or extradite allows an extension of jurisdiction to the State Party, makes us wonder whether it (the obligation) could be considered "universality by Convention" or, in other words, "a limited form of application of the universality principle". However, this is not the adequate context to discuss the

---

[45] There may be some discussion about this qualification. In spite of that, we believe that the continuous inclusion of the principle in various international Conventions establishes the existing feeling that the principle is customary law. Agreeing, **JORDAN J. PAUST**, "Above the Law: Unlawful Executive Authorizations Regarding Detainee Treatment, Secret Renditions, Domestic Spying, and Claims to Unchecked Executive Power", *Utah Law Review*, vol. 2007, issue 2, p. 367, note 51.

[46] Established by various international Conventions, the principle *aut dedere aut judicare* began with Huig de Groot's formulation *aut dedere aut punire* (extradite or punish), and was adapted because not always the alleged offenders are actually guilty. Thus, **ZDZISLAW GALICKI**, "The Obligation to Extradite or Prosecute ('aut dedere aut judicare') in International Law", Report of the International Law Commission. Fiftysixth session (3 May-4 June and 5 July-6 August 2004). Annex, p. 312, online at http://untreaty.un.org/ilc/reports/2004/2004report.htm, last visited September 2, 2008.

[47] Dealing with principles regarding extradition, article 24, paragraph 5, of the Convention establishes the applicability of the conditions provided by the domestic law of the requested Party.

[48] As an example, paragraph 3 of article 33 of the Portuguese Constitution allows for the extradition of Portuguese citizens only in conditions of reciprocity established by international convention, in cases of terrorism and organized crime, but on the condition the requesting State gives guaranties of a fair and equitable process. Also, according to paragraph 6 of the same article, no one is allowed to be extradited from Portugal when facing the possibility of death or irreversible harm to his/her physical integrity.

Such restrictions would not permit the extradition of a person – of any nationality – from Portugal, let's say, to China to face cybercrime charges, since China has been known to sentence hackers/cybercriminals to death (thus **MARCUS RANUM**, *Face-Off: Chinese Cyberattacks: Myth or Menace?* online at http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1321716,00.html, last visited September 2, 2008). One such case happened in Canada, with Chinese hacker Fang Yong being extradited to China to face the death penalty. See "Chinese Hacker Sentenced to Death for Embezzlement", *People's Daily*, online at http://english.people.com.cn/english/200006/13/eng20000613_42866.html, last visited September 2, 2008.

philosophic idea of whether the extension of jurisdiction provided by international conventions can be interpreted this way.

The Party requesting for an extradition should do so pursuant to the requirements and conditions of article 24, paragraphs 1 to 4 of the Convention. The requested Party should comply with paragraph 6 of the said article 24.

E. Positive jurisdiction conflicts

Finally, paragraph 5 of the article *sub judice* deals with positive jurisdiction conflicts. This type of conflict may occur because, sometimes, one offence (as described in the Convention) could target victims located in only one State;[49] whereas other times, it could target victims located in several States.[50]

This makes it quite normal that several Parties have jurisdiction over one given offence. To make proceedings efficient, the Convention establishes the possibility that the various Parties that claim jurisdiction over one offence consult with each other in order to determine the proper venue for prosecution.[51]

This would allow for an economy of means because, in some cases, it will be most effective for the States concerned to choose a single venue, whereas in others it may be best for one State to prosecute some of the alleged participants, while one or more other States prosecute another group of alleged offenders. However, since the obligation to consult is not absolute, taking place only "where appropriate", the effectiveness of this rule seems quite compromised.

---

49 This would be the case of Oleg Zezev, mentioned above, who – from Almaty, Kazakhstan – targeted a company (Bloomberg L.P.) in the USA.

50 This would be the case of David L. Smith, who was sentenced to 20 months in an US Federal Prison because he was the creator of Melissa, a virulent and widespread computer virus which was found on Friday, March 26, 1999. This virus spread all over the globe within just hours of the initial discovery, apparently spreading faster than any other virus before and disrupted personal computers and computer networks in business and government, in the USA and elsewhere. Melissa was initially distributed in an Internet discussion group called alt.sex. The virus was sent in a file bearing the name "list.doc", which supposedly contained a list of passwords for websites with sexual contents. As users downloaded the file and opened it in Microsoft Word, a macro inside the document executed and e-mailed the "list.doc" file to the first 50 people listed in the user's e-mail address book. See, **U.S. DEPARTMENT OF JUSTICE. NORTHERN DISTRICT OF OHIO**, "Florida Man Indicted for Causing Damage and Transmitting Threat to Former Employer's Computer System (February 7, 2006)", online at http://www.usdoj.gov/criminal/cybercrime/anchetaPlea.htm, last visited September 2, 2008. (For more information on the Melissa virus, see **KATRIN TOCHEVA**, **MIKKO HYPPONEN** and **SAMI RAUTIAINEN**, "F-Secure Virus Descriptions: Melissa", online at http://www.f-secure.com/v-descs/melissa.shtml, last visited September 2, 2008).

51 Thus, **SUSAN W. BRENNER** and **BERT-JAAP KOOPS**, "Approaches to Cybercrime Jurisdiction", p. 41.

II. Jurisdiction and Cyberworld threats

A. Cybercrime and Jurisdiction

The fact that – as mentioned above – article 22 of the Convention establishes jurisdiction based on territoriality and nationality grounds seems to actually create more problems than it solves. This is so because of the specific type of offence dealt with in the Convention: one person can send (upload) files whose contents are criminal from one computer in one country to a different computer (the server) in some other country and these files can be seen (downloaded) by viewers all over the world. In this case, where is the offence committed? In the country where the person lives and/or where the files are uploaded, in the country where the server is located or in the several countries where the criminal contents is actually seen? And, if we consider this last situation to be the correct interpretation, what if the viewer lives in a country where those particular contents are not criminal?

1. The Yahoo case

A good example of the complexity of the jurisdiction issues that arise in cyberworld is the Yahoo case. Based on the fact that the selling or exhibiting of racist objects, namely Nazi memorabilia, is illegal in France, the *Tribunal de Grande Instance de Paris*, in an *Ordonnance de Référé* of May 22, 2000, ordered Yahoo! Inc and its subsidiary Yahoo France not only to exclude French surfers from sales of Nazi memorabilia ("cesser... toute mise à disposition sur le territoire de la République à partir du site "Yahoo.com"), but also to destroy all the concerned files stored in their server ("détruire toute donnée informatique stockée directement ou indirectement sur son serveur").[52]

---

[52] For details, see the text of the sentence: **TRIBUNAL DE GRANDE INSTANCE DE PARIS**, *UEJF et Licra c/ Yahoo! Inc. et Yahoo France*, online at http://www.juriscom.net/txt/jurisfr/cti/tgiparis20000522.htm, last visited September 2, 2008. "UEJF" stands for *Union des Etudiants Juifs de France*; "Licra" stands for *Ligue Contre le Racisme et l'Antisémitisme*.

In this case, the files[53] were probably uploaded from an unknown source and were stored in a server in the United States. Then, one French court asserted jurisdiction over them because they could be seen in France and its contents was criminalized in France.

But the case does not end here. Dissatisfied with the sentence of the French court, Yahoo decided to file a declaratory judgment action in U.S. District Court in San Francisco, hoping to obtain a ruling that the French court's order could not be enforced against Yahoo in the United States. In its lawsuit, besides discussing computer technical matters regarding the (im)possibility of excluding some users of their site from some of the Web pages (those containing Nazi memorabilia), Yahoo maintained that allowing enforcement of the foreign court's order in the United States would violate the First Amendment. U.S. District Judge Jeremy Fogel of the Northern District of California ascertained jurisdiction over LICRA and UEJF (the French anti-racism associations), agreed with Yahoo regarding the violation of the First Amendment and entered a declaratory judgment in the company's favour.[54]

It was LICRA and UEJF's turn to be dissatisfied, this time with Judge Fogel's ruling, which led them to appeal to the 9th Circuit. Eventually, the matter came up for decision before an 11-judge panel of that court and the majority of the judges concluded that the district court had jurisdiction over the defendants (LICRA and UEJF), but the judgment of the district court was reversed.[55]

Could the Convention[56] help solve complex problems like the one presented in this case? It probably could! But would it?

---

53 The files to which the French court wanted no access from French citizens were digital copies of Adolph Hitler's "Mein Kampf" and of the book "Les protocoles des Sages de Sion", the supposed proceedings of a Zionist Congress supposedly held in Basel, Switzerland, in 1897. This book was thought – according to the research of Russian historian Vladimir Burtsev – to have been written by agents of the Okhrana, the secret police of Tsar Nicholas II, who himself seemed to have anti-Semitic ideas (thus, **JEAN-MARIE ALLAFORT**, "Les Protocoles des Sages de Sion", online at http://www.nuitdorient.com/n138.htm, last visited September 2, 2008). Further research from Russian historian Mikhail Lépekhine, done after the opening of Soviet archives to researchers, in 1992, showed that it was, in fact, the Russian forger Mathieu Golovinski who wrote the text while living in Paris. Thus, **ÉRIC CONAN**, "L'origine des Protocoles des sages de Sion", *L'Express*, 16/11/1999, online at http://www.phdn.org/antisem/protocoles/origines.html, last visited September 2, 2008.

54 *Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme*, N.D.Cal. 2001, Nov. 7, 2001, online at http://cyber.law.harvard.edu/is02/readings/yahoo-order.html, last visited September 2, 2008.

55 **UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT**, *Yahoo! Inc., a Delaware corporation, v. La Ligue Contre le Racisme et l'Antisemitisme, a French association; L'Union des Etudiants Juifs de France, a French association*, No. 01-17424, D.C. No. CV-00-21275-JF, online at http://caselaw.lp.findlaw.com/data2/circs/9th/0117424p.pdf, last visited September 2, 2008.

56 According to the Council of Europe website, the United States of America signed the Convention together with the majority of the Council of Europe members, on November 23, 2001, ratified the Convention on September 29, 2006, and it entered into force in the USA on January 1, 2007. (See online, http://conventions.coe.int.)

2. Controlling Law and International Cooperation

Immediately after establishing the jurisdiction principles mentioned above, the Convention proceeds to elaborate on international cooperation. Article 23, titled "General principles relating to international cooperation", creates an obligation for Parties to cooperate with each other in matters related with extradition (article 24), mutual assistance (article 25), spontaneous information (article 26) and some other details.

Good examples of international cooperation are the *Rome Labs* case and the *Tore Tvedt* case.

According to Appendix B of the Staff Statement of the US Senate's Permanent Subcommittee on Investigations, of June 5, 1996,[57] on March 28, 1994, computer systems administrators at Rome Air Development Center, Griffiss Air Force Base, New York, discovered that their network had been penetrated and compromised by an illegal wiretap computer program called a "Sniffer", which was covertly installed on computer networks by hackers to illegally collect user logons of authorized users. This program had been covertly installed on one of the systems connected to laboratory's network.

The intruders were found to be a pair of hackers calling themselves "Datastream Cowboy" and "Kuji," whose identities were unknown. "Datastream Cowboy", a 16-year old who enjoyed hacking into military networks, was located by an informant, who was able to provide a telephone number and address in the United Kingdom. US Air Force agents established a working relationship with New Scotland Yard agents and they arrested the hacker.[58] At the date of the report, "Datastream Cowboy" was pending prosecution in the UK. Three years later, Richard Pryce, *a.k.a.* "Datastream Cowboy", was fined with £1,200 for the intrusion.[59] Matthew Bevan, *a.k.a.* "Kuji", was also arrested, waited 18 months for a trial and was acquitted because it was judged not to be in the public interest to pursue the case.[60]

---

[57] **STAFF STATEMENT. U.S. SENATE. PERMANENT SUBCOMMITTEE ON INVESTIGATIONS**, *Security in Cyberspace*, June 5, 1996, Appendix B, online at http://fas.org/irp/congress/1996_hr/s960605b.htm, last visited September 2, 2008.

[58] **STAFF STATEMENT. U.S. SENATE. PERMANENT SUBCOMMITTEE ON INVESTIGATIONS**, *Security in Cyberspace*, online, quoted, p. 6. See, also, **GEORGE MOHAY**, **ALISON ANDERSON**, **BYRON COLLIE**, **OLIVIER DE VEL** and **RODNEY D. MCKEMMISH**, *Computer and Intrusion Forensics*, Norwood, MA, Artech House, Inc, 2003, pp. 308, 309, who use this as a case study for security in cyberspace.

[59] See the newspaper news published the day after the sentence was given in **DAVID GRAVES**, "'Datastream Cowboy', 19, fined £1,200 for hacking secret US computer systems", *Telegraph*, March 22, 1997,

The *Tore Tvedt* case dealt with the posting of racist and anti-Semitic propaganda on the Internet. Tore Tvedt, whose Web page was stored in a North American server, was the founder of the Norwegian far-right group Vigrid (an organization which professes a doctrine that mixes neo-Nazism, racial hatred and religion, claiming to worship Odin and other ancient Norse gods), and was considered responsible for the contents of the Web page – even if it was stored out of Norway's jurisdiction – and was sentenced by a Norwegian court to seventy-five days in jail with forty-five days suspended, plus two years of probation.[61]

In the *Rome Labs* case, the controlling law was that of the location where the actions in question occurred, the hacker's location. In the *Tvedt* case, however, the controlling law was that of the country in which the damage was said to have occurred. But both depended on international cooperation to be solved.

However, not all cases deal with good international cooperation. On October 10, 2001, the U.S. Department of Justice announced that Vasiliy Gorshkov, of Chelyabinsk, Russia, had been found guilty on 20 counts of conspiracy, various computer crimes and fraud, which made him face a maximum sentence of five years in prison for each count.[62]

After having discovered that some companies had suffered intrusions from hackers, the FBI created a shell company, called it Invita,[63] and eventually established contact with the hackers and lured them to the U.S. with employment opportunities. After long talks and some online testing, Vasiliy Gorshkov and Alexey Ivanov agreed to a face-to-face meeting in Seattle, where they were asked – by FBI undercover agents – about their hacking skills and assumed responsibility for various hacking incidents and activities. At the conclusion of the Invita meeting, the two men were arrested.[64]

---

online at http://www.telegraph.co.uk/htmlContent.jhtml?html=/archive/1997/03/22/nhack22.html, last visited September 2, 2008.

60 For a short story on Matthew Bevan, see **MARK WARD**, "History repeats for former hacker", *BBC News*, online at http://news.bbc.co.uk/2/hi/technology/4761985.stm, last visited September 2, 2008.

61 See the media report with comments at "Norwegian Jailed for Web Racism", *CNN*, Apr. 23, 2002, online at http://www.con.com/2002/WORLD/europe/04/23/norway.web/index.html, last visited September 2, 2008.

62 Thus, **U.S. DEPARTMENT OF JUSTICE. UNITED STATES ATTORNEY**, "Russian Computer Hacker Convicted by Jury", online at http://www.usdoj.gov/criminal/cybercrime/gorshkovconvict.htm, last visited September 2, 2008.

63 Describing the company, "High-tech net helped FBI snag alleged hackers", *USA Today*, 02/06/2002, online at http://www.usatoday.com/tech/news/2001-05-09-fbi-tech-sting.htm, last visited September 2, 2008, stated: "Invita Security looked like a typical Internet company: it had offices, computers, employees, even a secure computer system. The only thing missing was the customers."

64 **U.S. DEPARTMENT OF JUSTICE. UNITED STATES ATTORNEY**, "Russian Computer Hacker Convicted by Jury", online, quoted.

According to court filings,[65] the Department of Justice made several unsuccessful attempts to get Russian authorities to cooperate and seize the contents of the hackers' servers in Russia. The North American agents then accessed two servers in Russia where Gorshkov kept his data and downloaded over 1 Gigabyte of information. Subsequently, they obtained a search warrant to look at the downloaded files and got strong evidence of the men's computer hacking and fraud activities.[66]

This was one case where international cooperation did not function due to a lack of response from one of the sides. However, another case was reported where there was a will to cooperate but the law itself did not allow it.

Tens of millions of computers were affected in May, 2000, when the "Love Bug" virus swept the Internet. The virus was quickly traced back to the Philippines,[67] but then law enforcement officials ran into a problem, as the Philippines had no law against hacking.[68] Therefore, despite all the damage done,[69] nobody was ever prosecuted for the "Love Bug" virus. The United States wanted the extradition of the main suspect, [70] and there is an international extradition agreement between the United States and the Philippines. However, the lack of law against hacking in the Philippines made extradition impossible in this case.[71]

In the Invita case, the controlling law was that of the country in which the damage was said to have occurred. In the "Love Bug" case, however, the controlling law was that of the location where the actions in question occurred, the hacker's location. None of the cases depended on international cooperation to be solved. In fact, one was solved by hacking into

---

65 Reported by **ROBERT LEMOS**, "FBI "hack" raises global security concerns", *CNET News*, May 1, 2001, online at http://news.cnet.com/2100-1001-256811.html, last visited September 2, 2008.

66 **U.S. DEPARTMENT OF JUSTICE. UNITED STATES ATTORNEY**, "Russian Computer Hacker Convicted by Jury", online, quoted.

67 Supposedly to a Filipino computer student who wrote a thesis on stealing passwords from the Internet. "Love Bug revenge theory", *BBC News*, May 10, 2000, online at http://news.bbc.co.uk/2/hi/science/nature/743082.stm, last visited September 2, 2008.

68 See "Philippine investigators detain man in search for 'Love Bug' creator", *CNN*, May 8, 2000, online at http://archives.cnn.com/2000/TECH/computing/05/08/ilove.you.02/index.html, last visited September 2, 2008.

69 In the UK alone, British Telecom, Vodafone, Barclays, Scottish Power and Ford UK were among the giant firms affected, together with universities and many companies of variable size. "'Love Bug' bites UK", *BBC News*, May 4, 2000, online at http://news.bbc.co.uk/2/hi/uk_news/736080.stm, last visited September 2, 2008.

70 See, *inter alia*, "Suspected hacker may face extradition requests", *CNN*, May 9, 2000, online at http://transcripts.cnn.com/2000/LAW/05/09/internat.hacking.law/index.html, last visited September 2, 2008.

71 Thus, **SETH MYDANS**, "Philippine Prosecutors Release 'Love Bug' Suspect", *The New York Times*, May 10, 2000, online at http://partners.nytimes.com/library/tech/00/05/biztech/articles/10virus.html, last visited September 2. 2008.

the servers in another country, whereas the other was not solved at all due to an absence of legislation. Sometimes there is a will, but there is no way!

3. Jurisdiction Issues

Cybercrime is so broad and can be so complex that becomes very difficult to investigate. And jurisdiction adds to the complexity of investigating a technological matter. [72] This difficulty becomes more evident when dealing with international jurisdiction.

Doctrine considers jurisdiction as defining three levels of authority: ① the authority to prescribe (the capacity to establish and prescribe criminal and regulatory sanctions, normally prerogative of a government), ② the authority to judge (the competence to hear disputes, normally prerogative of courts), and ③ the authority to enforce (the capacity to compel compliance or to punish noncompliance with its laws, regulations, orders, and judgments, as well as the capacity to investigate suspect behaviours, both normally also prerogative of a government).[73]

The Convention on Cybercrime points the way toward cooperation with respect to criminalizing certain behaviours and pursuing those responsible. It does not, however, resolve the issues of international jurisdiction. The investigation of an international crime will always have to depend on the good will of the third country, or else there is no investigation. However, even if the Convention relies heavily on international cooperation, sometimes – as we have seen – this is not enough to take the investigation to an end. We are, therefore, forced to conclude that the Convention is short on giving States the necessary weapons to fight this type of crime.

As an attempt to remedy this deficiency, we would propose three amendments to the Convention: ① that the consultations of which we have spoken above were not to take place

---

[72] Regarding the complexity of investigation, see **DAN KOENIG**, "Investigation of Cybercrime and Technology-related Crime", *National Executive Institute Associates*, online at http://www.neiassociates.org/cybercrime.htm, last visited September 2, 2008. Peter Stephenson, *Investigating Computer-Related Crime: A Handbook for Corporate Investigators*, Boca Raton, FL, CRC Press, 1999, p. 13, adds that most organizations are not equipped to investigate computer crime.

[73] Thus, *inter alia*, **SUSAN W. BRENNER** and **BERT-JAAP KOOPS**, "Approaches to Cybercrime Jurisdiction", p. 4. According to **IAN BROWNLIE**, *Principles of Public International Law*, 5th ed., Oxford, University Press, 2002 (1998), p. 58, law-making capabilities are one of the factors that determine the coexistence between nations.

"where appropriate", but that they would be established as an obligation;[74] ② that the Convention itself be effectively considered as an extradition convention between the Parties;[75] and ③ that the Convention be amended (or supplemented by additional protocol) to include an internal mechanism that allows police investigators from one Party to perform their work online in another Party, subject only to an informal communication to the authorities in the other Party. [76]

---

[74] Should the Convention create an obligation to consult – instead of merely allowing for this consultation, as it does with the current wording – this obligation would have the advantage of permitting the determination of the most appropriate venue for persecution, together with an economy of means that would help the international community in not leaving any crime unpunished.

[75] We are aware that paragraph 3 of article 24, allows a Party to consider the Convention as legal basis for extradition. However, the wording of the Convention is weak. The party "may consider" the Convention as legal basis for extradition, but is allowed to consider the opposite. A stronger wording would, in our view, be recommendable.

[76] The formal request to the other Party's authorities can be useful when dealing with apprehending people or computers. Nevertheless, in cybercrime, sometimes the investigator has to follow the path of the perpetrator of the offence and may find himself messing with a computer that is physically in a place where he does not have jurisdiction. A formal request would probably result in losing the evidence. However, an informal communication would allow the investigator to pursue the investigation in time.

In the Invita case, for example, if the North American agents had not entered the Russian servers without permission, there would have been no way to prove that the statements both hackers made at the Seattle interview were true, because it was expected that, as soon as the two suspects' counterparts in Russia found out about the arrests, they would have destroyed the data.

The data copied from the Russian computers had large databases of credit card information (more than 56,000 credit cards) that were stolen from Internet Service Providers. The two Russian computers also had stolen bank account and other personal financial information of customers of online banking at a couple of North American banks. Should the research have waited for a formal answer ... there would have been no proof and the information would still be usable by others. See **U.S. DEPARTMENT OF JUSTICE. UNITED STATES ATTORNEY**, "Russian Computer Hacker Convicted by Jury", online, quoted.

B. Cyberterrorism and Jurisdiction

1. To Be or Not To Be

Cyberterrorism conjures up images of fierce terrorists unleashing catastrophic attacks against computer networks, creating chaos, and paralyzing entire nations. A frightening scenario indeed, but how likely is it to occur? From people in denial to people in distress, opinions come in all flavours.

On the denial corner, strong statements make the day. "There is no such thing as cyberterrorism – no instance of anyone ever having been killed by a terrorist (or anyone else) using a computer" says an editor of one monthly magazine from Washington, DC, USA.[77] Besides arguing that no cyberattack has ever been attempted by terrorists,[78] the main line of reasoning of those in this field is that terrorist organizations usually follow the least resistance path and, therefore, are bound to prefer a cheaper and easier alternative to cyberattacks: physical attacks.[79] Yet, are physical attacks now easier and cheaper?

On the opposite corner, statements come in no weaker form. Carnegie Mellon University computer scientist Roy Maxion is reported to have written, in 2001, to President George W. Bush warning him about the fact that the United States was at grave risk of a cyberattack that could devastate the public mind and the nation's economy more broadly than the September 11 attacks.[80] And the reasoning for this extreme position is based on the findings that al Qaeda operators spent time learning about how to disrupt critical infrastructures through the Internet and had plans to put that knowledge to use.[81] Yet, are things really this bad?

If it is true that they are out there, what is then the measure of danger that cyberterrorists really embody? [82] The reality may have been grasped in July 2002, as the

---

77 **JOSHUA GREEN**, "The Myth of Cyberterrorism", *Washington Monthly*, November 2002, online at http://www.washingtonmonthly.com/features/2001/0211.green.html, last visited September 2, 2008.

78 *Ibidem.*

79 Referred by **SEAN P. GORMAN**, *Networks, Security and Complexity: The role of Public Policy in Critical Infrastructure Protection*, Glos, UK, Edward Elgar Publishing Limited, 2005, p. 11.

80 See **DAN FITZPATRICK**, "Cybersecurity expert warns of post-9/11 vulnerability", *Global Security*, September 9, 2003, online at http://www.globalsecurity.org/org/news/2003/030909-cyber01.htm, last visited September 2, 2008.

81 See **BARTON GELLMAN**, "Cyber-Attacks by Al Qaeda Feared", *Washington Post*, June 27, 2002, page A01, online at http://www.crime-research.org/library/Barton.htm, last visited September 2, 2008.

82 **FRED COHEN**, "Cyber-Risks and Critical Infrastructures" in Alan O'Day (ed.), *Cyberterrorism*, pp. 1-8, lists several critical infrastructures and mentions nightmare scenarios for each one. He then proceeds to solve

United States Naval War College, working in conjunction with Gartner Research, conducted what they called a "digital Pearl Harbour" simulation. According to the conclusions of this simulation, "a group of hackers couldn't single-handedly bring down the United States' national data infrastructure, but a terrorist team would be able to do significant localized damage to U.S. systems."[83]

The analysts concluded that it would be possible to inflict some serious harm to the US data and physical infrastructure systems, but it would require a syndicate with significant resources, including $200 million, country-level intelligence and five years of preparation time. [84]

The conclusions then show that a cyberattack on the United States is possible, but would require huge planning and a great amount of financing. Considering the above mentioned *Rome Labs* case, if one 16-year old British boy – with £ 750 worth of equipment[85] – was able to intrude a network connected to the US military, the funding requirement is probably overstated.

Cyberterrorists might not be menacing to kill people directly, as a traditional terrorist attack normally does, but one cyberattack could make life very, very difficult, maybe even destroying or severely damaging the complete economical and social system of one country. We thus conclude that cyberterrorism is definitely a real threat which, unfortunately, is here to stay. And, since the chain of terrorist events after September 11, 2001 shows terrorists to have diversified their targets, we should therefore not overlook the possibility of a cyberattack targeting some other less prepared country than the USA.

If an ounce of prevention is worth a pound of cure, we should learn at least one lesson from the catastrophic terrorism actions perpetrated in New York, Madrid and London: terrorists did not attack from a distance. If a cyberattack is to take place in our countries, it can be masterminded elsewhere, but will probably be executed from within our own networks.

---

every one of those scenarios within a framework ranging from only a few hours to a few days, thus showing that a cyberattack would not create havoc for long. As he mentions the Internet, for instance, he states that there are hundreds of thousands of trained experts that could recreate a functional Internet "in a matter of days" (p. 8). He recognizes, by that, the possibility of one such attack.

83 **MARGARET KANE**, "U.S. vulnerable to data sneak attack", *CNET News*, August 13, 2002 11, online at http://news.cnet.com/2100-1017-949605.html, last visited September 2, 2008.

84 *Ibidem.*

85 Thus, **DAVID GRAVES**, "'Datastream Cowboy', 19, fined £1,200 for hacking secret US computer systems", online, quoted.

2. Hackers, Crackers, Terrorists and Jurisdiction Issues

Hackers tend to be more of a nuisance than a danger. Most of the time, they try unauthorized access to networks for the fun of it, for the challenge, or to put networks to a test. [86] Crackers, however, are criminal hackers that also try unauthorized access to networks, but have malicious intents.[87] Cyberterrorists are people that use cyberterror to achieve political or social change. [88]

Because their motivation and goal is so much different from those of crackers and terrorists, hackers are not likely to either become terrorists or be directly employed by them. For trust reasons, it is not likely that terrorists would hire crackers. But it is not impossible for terrorists to gain hacking skills.[89]

Whatever motivation or goal leads one person (or a group) to hack into a network system, be it hacking, cracking or terrorism, the same jurisdiction problems are present to the investigator and to the judge. Obtaining proof of the action, detaining the suspects and presenting them to a court can only to be achieved with quick reaction and the appropriate international tools. This author believes that international cooperation is the way to achieve this goal; however, he also finds that existing international tools fall short on making international cooperation injunctive.

---

86 **ANDREW MICHAEL COLARIK**, *Cyber Terrorism. Political and Economic Implications*, Hershey / London / Melbourne / Singapore, Idea Group Publishing, 2006, pp. 37-39, discusses the actions normally attributed to hackers, stating (p. 37) that some have even published their findings, either in academic or nonacademic venues.

87 *Idem*, pp. 40-42.

88 *Idem*, p. 46, states that because no legislatively defined meaning of cyberterrorism exists, "the domain is open to debate, dispute, and ultimately, ambiguity." In this text we are not trying to establish a definitive definition for cyberterrorism, for which reason we employed vague wording, as did **DOROTHY E. DENNING**, "Cyberterrorism", Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services, U.S. House of Representatives, May 23, 2000, online at http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html, last visited September 2, 2008, when she wrote: "Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives."

89 Thus, **AYN EMBAR-SEDDON**, "Cyberterrorism: Are We Under Siege?" p. 15. **A. M. COLARIK**, *Cyber Terrorism*, p. 51, states "Cyberterrorists exist today. The Osama bin Laden Crew is a group of self-proclaimed cyberjihadists", and proceeds to mention force multiplier tasks that cyberterrorists are supposed to be accomplishing.

C. The applicability of Article 22 to cyberterrorism cases

As a threat, cyberterrorism would probably not justify a convention to deal with it. The explicit inclusion of cyberterrorism in the Convention on Cybercrime by means of an additional protocol would probably suffice. Whatever the choice, it is, however, this author's belief that to fight cyberterrorism there is no need for a definition. The broad acceptance of the 1988 Rome Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation shows there is no need to use "scare words" in order to reach consensus. In fact, it was probably due to the lack of such words that the Rome Convention was so successfully adopted. Thus, given the fear of terrorism in our society, an Additional Protocol to the Convention – either detailing some offences that would be considered cyberterrorism or specifying when the offences established in the Convention should be considered more than just cybercrimes – should be enough.[90]

The effectiveness of this Protocol, as well as of the Convention itself, would however depend on the number of States that ratify them. The fact that the United States of America has ratified the Convention, in accordance with its article 36, paragraph 1, *in fine*, is a sign that major non-Council of Europe Member States will be willing to cooperate with Member States in the fight against cybercrime and, obviously, against cyberterrorism. Yet, although the Convention entered into force in July 1, 2004, key Member States of the COE – *v.g.* Germany, Russia, United Kingdom, Spain, Austria, as well as the author's own country, Portugal – have not (as of September 1, 2008) ratified the Convention, a situation that can spawn great concern.

Concluding Remarks

Jurisdiction, or the lack of it, seems to be the most problematic issue in the fight against cybercrime and cyberterrorism. The fact that cyberattacks can come from anywhere in the world makes investigation, producing evidence and taking the offenders to court an immense task that can only be achieved through international cooperation.

---

[90] This Protocol could also include the amendments referred above (Part II, section A, subsection 3) regarding consultation between the Parties, extradition rules and the inclusion of a mechanism to allow police investigators to perform their search online, subject only to an informal communication to the local authorities.

The Convention on Cybercrime was designed to help accomplish the goal of reducing and/or tearing down the difficulties of the fight against cybercrime. Still, it shows itself to be insufficient because international collaboration in not injunctive and there are no rules to unload the burden of formality from the work of police specialists in charge of investigating international cybercrime/cyberterrorism cases.

Furthermore, the fact that key Member States of the Council of Europe are taking their time to ratify the Convention also leaves a bitter notion of lack of interest in cybercrime, one type of crime that is becoming increasingly important for companies all over the world. Let's hope our countries don't wake up too late. It is easy to be wise after the event!

As a final note, we would like to say that, given the path towards catastrophism and indiscriminate attack on human lives taken by modern day terrorism, we would consider possible and positive the inclusion of terrorism in the list of international crimes against humanity – in accordance with *littera k* of number 1 of article 7 of the Rome Statute of the International Criminal Court (ICC) – which would entitle States to have universal jurisdiction to apprehend terrorist agents, although jurisdiction to prosecute would be given to the International Criminal Court.

Thus, since, in the case of international conventions, the authority to prescribe still rests with the government of the State Party – because no State is forced into being a Party to a Convention and all States still have the right to sign (or not) and ratify (or not) any given Convention – the governments of the Member States concerned would only forfeit the authority to judge to the International Criminal Court. All States would keep the authority to prescribe, both domestically and by means of ratification of conventions, and the authority to enforce, should the International Criminal Court convict the agents.