Towards a Global Convention against Cybercrime*

Joachim Vogel**

Es un honor y un placer para mí el poder hablar en este Primer Congreso Internacional de Derecho Penal en Guadalajara/Mexico. Quisiera agradecer a los organizadores por la invitación y organización, particularmente al Grupo Mexicano de la Asociación Internacional de Derecho Penal y a su presidente D. Espinoza de los Monteros. Entrando en el tema „Hacia una Convención Global contra la Cibercriminalidad", voy a proceder en tres pasos: Primero, presentaré un marco teórico, subrayando tendencias significativas en la materia del derecho penal contra la cibercriminalidad (I). Segundo, analizaré la legislación vigente y unos proyectos futuros en Europa, región muy activa y innovadora en la lucha contra la cibercriminalidad (II). Tercero y, finalmente, estudiaré las perspectivas para una convención global contra la cibercriminalidad (III). En mi opinion, ha llegado el momento de elaborar y negociar tal instrumento. En este proceso, la Asociación Internacional de Derecho Penal podría contribuir valiosamente. Permítanme continuar en inglés.

1. During the 17th International Congress of Penal Law held in Beijing 2004, the problem of cybercrime was discussed in Round Table II. My German colleague Sieber – director of the famous Max-Planck-Institute of Foreign and International Criminal Law in Freiburg/Germany and certainly on of the world's leading experts in the field of cybercrime – presented a landmark General Report on „Computer Crimes, Cyber-Terrorism, Child Pornography and Financial Crimes"[1]. Sieber's central argument is that the emerging information society and its vulnerability pose, as a matter of fact, new risks and, as a matter of law, new challenges for the criminal justice system[2]. I do concur and would like to focus on six major legal challenges (1.-6.): definition; jurisdiction; investigation; international cooperation; public-private partnerships; and prevention.

1.1. The first legal challenge is to adequately define cyber-crime and specific cyber offences. Cyber technology is rapidly developing and ever changing, and so are methods and patterns of harmful, abusive activities which relate to information systems. Therefore, legal instruments on cybercrime must not define that concept in too rigid, too determinate terms; we need a definitional framework with a certain amount of openness, flexibility and even vagueness. The legal challenge arising here for a criminal justice system is to balance that need with the legal requirement of foreseeability and the constitutional prohibition of too vague, essentially indeterminate offences.

There is no universally accepted definition of cybercrime as such. Literally, cybercrime means crime related to the cyberspace, in particular computers, computer networks and the internet. However, cybercrime is no longer what it used to be: computer and internet crime. Nowadays, the essential concepts are "information systems" and "data". Information system is commonly defined as any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data[3]. And data are any representation of facts, information or concepts in a form suitable for processing in an information system, including a program suitable to cause an information system to perform a function[4]. Under these definitions, a personal digital assistant is certainly an information system, and probably also a modern car or a

---

* Paper presented at the First World Conference on Penal Law, 19-23 November 2007, in Guadalajara/Mexico, with subsequent modifications.

** Dr jur, Dean of the Faculty of Law and Chair of International and European Criminal Law, University of Tuebingen, Germany, Judge at the Superior Regional Court, Stuttgart/Germany. Contact via e-mail vogel@jura.uni-tuebingen.de. Internet: http://www.eurocrim.org.

1 See Sieber, in: Spinellis (ed.), Computer Crimes, Cyber-Terrorism, Child Pornography and Financial Crimes. Reports presented to the Preparatory Colloquium for the Round Table II of the 17th International Congress of Penal Law (Beijing, 2004), Athens 2004, p. 11-50.

2 Sieber, loc. cit., p. 14-21.

3 See Art. 1(a) Convention on Cybercrime.

4 See Art. 1(b) Convention on Cybercrime.

state-of-the-art TV set. In particular, the borders between information and telecommunication systems become blurred. A complex mobile telephone is certainly an information system processing data, and offences related to mobile telephones may well be included in a modern cybercrime definition.

Accordingly, the scope of specific cyber offences is not at all limited to manipulating or sabotaging computers. Rather, modern cyber offences refer to a wide variety of harmful behavior linked with information systems and/or data, and – more concretely – include[5]

- offences against the confidentiality, integrity and availability of information systems and data, in particular illegal access to systems or data, illegal interception of data, and illegal interference with systems and data,
- computer-related offences, that is to say offences similar to traditional offences but committed through or by means of an information system, e. g. computer-related fraud or forgery, but also computer-related harassment etc.,
- content-related offences, e. g. dissemination of child pornography or hate speech through information systems, and of course
- offences related to the infringements of copyright and related rights, e. g. software, film or music piracy.

Recently, further offences have been discussed such as serious cases of spamming, identity theft, phishing and pharming and – of course – cyber terrorism. However, it is unclear whether these offences can (and should) be integrated into the structure just outlined. For example, cyber-terrorism might be a large-scale attack against an information system (e. g. if terrorists would attack, say, information systems essential for international capital markets so that these markets break down), a computer-related offence (e. g. if terrorist would take over an information system managing a nuclear facility and trigger a nuclear meltdown) or a content-related offence (e. g. if terrorist disseminate propaganda or, say, blueprints for bombs via internet) but hardly can be spelt out as a separate category or offence.

1.2. Cybercrime occurs in cyberspace – that is to say in a virtual and global space more or less independent from traditional states: Criminal hate speech may be drafted in State X, transmitted through State Y to a server in State Z, and downloaded by the global internet community in any state of the world. The global character of cybercrime constitutes a major legal challenge for national criminal justice systems and their jurisdiction traditionally based on the territoriality principle and only supplemented by other principles such as active personality (i. e. jurisdiction over offences committed by own nationals abroad), passive personality (i. e. jurisdiction over offences against own nationals). At first glance, a solution might be to apply a universal jurisdiction principle as the natural complement to the global character of cybercrime. However, problems of dual criminality and even dual illegality arise as it is illustrated by the Toeben Case decided by the German Federal Supreme Court in 1999[6]: Mr Toeben, an Australian national, created a website in Australia in English language which included a statement that the Shoa never happened – the so-called "Auschwitz denial". The website could be accessed in Germany and was indeed accessed by German neo-Nazis. Under German law, the "Auschwitz denial" is (for obvious historical and political reasons) a criminal offence. The Supreme Court convicted Mr Toeben of that offence and held that Germany had jurisdiction under the territoriality principle because the website could be accessed here so that the result of the offence (under German law: disturbing the public peace) occurred here. In applying German – and only German – law, the court did not investigate whether Mr Toeben's conduct was criminal or illegal under Australian

5 See Art. 2-10 Convention on Cybercrime.

6 German Federal Supreme Court (Bundesgerichtshof), Judgement of 12.12.2000 – 1 StR 184/00 (Case Frederick Toeben), Decisions vol. 46 (2001), p. 221-235.

law. But at that time, Australian law did not criminalize the "Auschwitz denial" as such, and Mr Toeben might have even invoked the fundamental right to free speech under Australian constitutional law (whereas according to German constitutional doctrine, the dissemination of false facts is not protected by that right). In other words: The alleged criminal act occurred in a place where the conduct was probably legal, at least not criminal. To ignore that circumstance (as the German Supreme Court did) seems obviously problematic – consider the hypothetical counter-examples of a German internet beer advertisement which might be accessed in an Islamic country where any advertisement of alcoholic beverages is a criminal offence, or of a German internet blog critical of a dictatorship in the Far East when the blog is accessible in the respective country where such criticism is high treason and a capital offence. It seems that some degree of legal harmonization is necessary for legitimate extraterritorial or even universal jurisdiction.

1.3. Investigating cybercrime in a data processing environment is, of course, a factual challenge because the investigation objects – information systems and data – and methods differ widely from traditional objects – e. g. a crime scene – and methods. However, there is also the legal challenge to balance the need for cybercrime-specific investigation powers and fundamental "cyber rights" such as data privacy and data protection.

Investigation powers which are more or less uncontroversial because they are basically cyber-specific equivalents of traditional investigation measures include

- expedited preservation of stored computer and also traffic data, the so-called "quick freeze procedure" to ensure that cybercrime investigations do not fail simply because data were deleted during the (often lengthy and complex) investigation process,
- search and seizure of stored computer and also traffic data, and
- real-time collection of traffic data and interception of content data (provided that the general requirements of an interception of telecommunications are fulfilled).

In contrast, controversial investigation powers do not fit into the traditional set of instruments and tend to be in conflict with traditional legal principles. A power hotly debated in Germany[7] is the use of remote forensic software to carry out remote data search procedures, record VoIP communications, log keystrokes and passwords and identify IP addresses used or contacted by suspects: Is such a total control of an information system and of its users' information behavior proportional? And even if a need for secret investigations (to avoid the detection and destruction of ongoing investigations) must be recognized on a case-to-case-basis, a democratic state should adhere to the principle that secret police action should remain an exception. – An instrument also hotly debated in Europe is data retention[8]: European telecommunication service providers are obliged to retain any and anybody's traffic data for at least six months, and state authorities can use these data to investigate and prosecute at least serious offences. But is such a total control of a whole population's telecommunication behavior without specific suspicion proportional, and does it infringe on the right to data privacy? – Similarily, the often mentioned production order, a legally binding order to produce specific data, among them passwords, encryption codes etc., may be in conflict with the fundamental right of a suspect against self-incrimination. The solution that producers of encryption software are legally obliged to build in "backdoors" and make them

7 On 01.01.2009, an amendment to the German Act on the Federal Criminal Police Office (Bundeskriminalamt-gesetz) went into force permitting the use of remote forensic software in order to prevent imminent attacks by international terrorist groups. A constitutional appeal against that amendment is still pending before the German Federal Constitutional Court.

8 See the 2006 European Union Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (…), O. J. No. L 105 of 13.04.2006, p. 54: Any telecommunication service provider – including internet providers – is legally obliged to store traffic data of any telecommunication – including any use of the internet – for at least six months in order to facilitate the investigation and prosecution of serious crime.

available to state authorities potentially damages the trust needed for a widespread use of the internet.

1.4. The need for international cooperation in combating cybercrime is evident due to the very nature of cyberspace itself. In particular, its borderless nature enables individuals and groups to exploit "loopholes of jurisdiction" and take advantage of specific countries' difficulties to respond adequately, due to legal reasons or because authorities do not have the necessary technical expertise or resources to address cybercrime efficiently. Therefore, cooperation, coordination and (minimum) harmonisation are needed: Cooperation includes extradition – at least serious cyber offences should be extraditable offences – and mutual legal assistance – with a focus on cyber-specific investigation measures –. Cybercrime investigations often involve two or more states so that a coordination mechanism – which state should do what? – is useful or even indispensable. And without some minimum harmonisation of substantive and also procedural law, cooperation efforts are bound to fail. On a more practical note, it might also be considered to establish a global cyber identity for internet users.

1.5. A further legal challenge results from the fact that states are, vis-à-vis the internet, actors of limited power and capacity so that there is a need of public-private partnerships in fighting cybercrime. The development of modern information and communication technologies has been and is largely controlled by private actors. The internet has been constructed as a private and non-hierarchical global network without specific location and definitely not under state control. The sheer volume of today's internet communication makes it an impossible task for state authorities with limited resources to „check the web". And "normal" police and prosecution authorities often lack the technological experience and capacity to investigate and prosecute efficiently in a complex data-processing environment. Therefore, criminal justice systems depend on the private sector – the civil society and the economy, in particular the information and communication technology industry and service providers of all kinds — for an efficient investigation and prosecution of cybercrimes. Without active participation of the private sector, it is hardly possible, for example, to detect the whole spectrum of child pornography in the internet and trace it to its distributors and, in the end, producers.

Public-private partnerships against cybercrime can be formed on a voluntary basis. Indeed, there is quite a potential for voluntary cooperation: Public and private sector have a joint interest in developing methods to prevent harm resulting from cybercrime. State authorities and private companies carry out threat assessments, establish prevention programs and develop technical solutions. On the other hand, it is true that private actors are naturally reluctant to share information, expertise and best practices with state authorities because they want to protect their business models, secrets and also the customer trust. Nevertheless, certain types of voluntary public-private partnerships against cybercrime have been developing during the last years. They include

- operational cooperation in specific cases,
- blocking of websites containing illegal content such as child pornography or hate speech,
- private self-regulation through codes of conduct,
- sharing of necessary and relevant information across the private and public sector, and
- setting up networks of contact points in both the private and the public sector.

An instructive example of a voluntary private-public partnership is the so-called „Mikado operation" which took place in Germany in 2006[9]: In 2004, a German TV station had identified a

9 Critical account by Schnabel, Das "Mikado-Prinzip", in: Datenschutz und Datensicherheit vol. 31 (2007), p. 426-430.

website offering the download of child pornography following payment of 79,99 US-$ through an internet credit card transaction into a specific account. In order to investigate and prosecute persons who downloaded and, consequently, possessed child pornography (which is a criminal offence under German law), a public prosecutor asked 22 German credit card firms to scan all their clients' credit card transactions from 2004 and identify those clients who had transferred 79,99 US-$ into the specific account. The credit card firms cooperated on a voluntary basis, and billions of credit card transactions by millions of credit card holders were checked without their consent. Indeed, 322 persons were identified who had transferred the exact amount into the specific account. The authorities applied for search and seizure orders against these persons, and in fact many of them had downloaded child pornography. It is still in dispute whether state authorities and/or the cooperating credit card firms acted legally under current German law.

Of course, states may also decide to oblige private actors to cooperate with state authorities. Indeed, we see various legal duties to cooperate with the state in the fight against cybercrime. These duties include

- duties to report cybercrimes to state authorities,
- duties to render support in specific investigations, in particular through production of specific data, passwords and/or subscriber information,
- duties to provide „back doors" into information systems which may be used by state authorities without knowledge of either the system provider or the user,
- duties of data preservation and data retention[10],
- duties to provide state authorities with encryption keys; and
- corporate governance duties to prevent and, as case may be, investigate and report cybercrimes committed within the company.

Although public-private partnerships against cybercrime are a „hot" political topic and much endorsed by – among others – the European Commission, they are not beyond legal and political doubt. Cases like the German „Mikado operation" raise questions of proportionality, but also of legality – indeed, it was quite doubtful whether the credit card companies cooperation was in conformity with German data and client protection law, and there are appeals pending both of persons who were, in the end, identified and convicted, and of persons whose credit card transactions were checked without any result. The traffic data retention obligation stipulated by the European Union has come under constitutional legal attack for example in Germany because of an infringement on the right of data privacy and on the principle of proportionality: Is it proportional to treat a whole population as potentially suspect and store traffic data which may be highly sensitive (for example if a lawyer makes telephone calls or sends e-mails to prepare a criminal defence)? Speaking more generally, it is a difficult question whether industry and civil society should be made „agents of law enforcement authorities" which might create a general and unhealthy atmosphere of control and mistrust throughout a whole society.

1.6. Finally, prevention is a major legal challenge in the field of cybercrime[11]. State authorities cannot investigate and prosecute more than a tiny fraction of cybercrime, and cyber security depends almost exclusively on prevention. Indeed, what we have seen recently is a paradigm shift from the fight against cybercrime towards a more general approach of enhancing cyber security, and criminal law is one of many tools to achieve that aim. Insofar, the modern focus is on

- „hardening" information systems and, in particular, critical and vulnerable information infrastructure against criminal attacks,

10 See supra note 11.

11 The prevention aspect is highlighted in the European Commission Communication „Towards a general policy on the fight against cyber crime", see infra note 25.

- protecting cyber communication by encryption, electronic signatures etc., and
- raising the awareness of the civil society towards cybercrime, in particular towards content-related offences such as child pornography or hate speech. Indeed, the check-the-web-attitude has already reached civil societies, and civil organizations have emerged which, for example, identify child pornography in the internet, create data bases and share their information with state authorities.

However, a cyber space free of cybercrime is an unrealistic aim, and we should bear in mind that security enhancement and preventive control must not infringe on human and fundamental rights, in particular the right to privacy and free speech.

2. Let me now turn to the European efforts to establish a common legal framework against cybercrime. Until recently, the major European player in the field of action against cybercrime has been the Strasbourg-based Council of Europe (CoE) (1.). Nowadays, the initiative has shifted to the Brussels-based European Union (EU), both in legislation and practice (2.). In a way, a European anti-cybercrime area has been created which might play a model role for the future global development.

2.1. The 2001 CoE's Convention on Cybercrime[12] must be regarded as a historic milestone in the fight against cybercrime and – for the time being – as the leading and reference international instrument on cybercrime[13]. Indeed, the CoE member states include non-European states (e. g. post-Soviet states in Middle and Eastern Asia), and the convention is even open for accession to non-member states and has, indeed, been acceded by some, among them the United States of America. The convention entered into force on 1 July 2004; by today, 24 states had ratified it, while 22 states had signed, but not yet ratified it. The convention is supplemented by the 2003 Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems[14.]

In substance, the convention uses technology-neutral language so that it applies and covers both current and future technologies. Formally, it consists of four chapters.

Chapter I (Art. 1) on the use of terms includes definitions on computer systems, computer data, service providers and traffic data which have become an international standard.

Chapter II (Art. 2-22) on measures to be taken at the national level includes sections on substantive criminal law, procedural law and jurisdiction. The section on substantive criminal law (Art. 2-13) identifies offences against the confidentiality, integrity and availability of computer data and systems (such as illegal access, illegal interception, data interference, system interference and misuse of devices), computer-related offences (such as forgery and fraud), content-related offences (such as child pornography and, in the Additional Protocol, certain forms of hate speech), and offences related to infringements of copyright and related rights. By ratifying or acceding to the convention, states agree to ensure that their domestic laws criminalize the conducts described in the section but may exclude petty or insignificant misconduct from the offences it defines. Offences must be committed "without right", referring to conduct undertaken without authority or conduct not covered by established legal defences, excuses, justifications or relevant principles under domestic law; the definitions are not intended to criminalize legitimate and common activities inherent in the design of systems and networks, or legitimate operating or commercial practices. Criminal liability requires intention which may be understood as acting wilfully and/or knowingly and is left to national interpretation; additional specific intentional elements apply to certain offences (for instance to computer-related fraud with the requirement of

12 Council of Europe Treaty Series No. 185 of 23.11.2001.

13 In the World Summit on the Information Society (WSIS) Tunis Agenda for the Information Society of 18.11.2005, governments recognized the convention as a regional initiative (para. 40).

14 Council of Europe Treaty Series No. 189 of 28.01.2003.

fraudulent or dishonest intent of procuring economic benefit). The section on procedural law (Art. 14-21) applies to the cyber offences defined in Art. 2-11, but also to criminal investigations of a criminal offence of whatever kind if it has been committed by means of a computer system, and to the collection of evidence in electronic form relating to any criminal offence. There are provisions on expedited preservation of stored computer data, expedited preservation and partial disclosure of traffic data, production orders, search and seizure of stored computer data, real-time collection of traffic data, and interception of content data. The section on jurisdiction (Art. 22) is based on the territoriality and active personality principle.

Chapter III (Art. 23-35) on international cooperation includes general principles relating to international cooperation, extradition, mutual assistance and spontaneous information. The chapter contains procedures pertaining to requests for mutual assistance in the absence of applicable international agreements, and to confidentiality and limitation on use, including specific provisions on mutual assistance regarding provisional measures, mutual assistance regarding investigative powers, and a provision for a 24/7 network (Art. 35).

Chapter IV (Art. 36-48) on final provisions contains the final clauses, mainly in accordance with standard provisions in Council of Europe treaties.

In fact, the convention tackles many of the legal challenges mentioned in Part I of this presentation. However, cybercrime is so dynamic that the convention is already partly outdated. Recent cybercrime phenomena such as

- attacks on critical infrastructure and cyber terrorism,
- denial of service attacks and massive "spamming",
- the so-called „phishing" and „pharming" of passwords and
- identity theft

are not adequately dealt with. The convention focuses on cybercrime and neglects the more comprehensive aspect of cyber security including technical prevention, organizational aspects and the public-private partnerships in cyber law enforcement.

2.2. Since a decade, combating cybercrime and promoting cyber security has been a major political aim of the EU. On 26 Januar 2001, the European Commission presented a communication on "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime"[15]. The communication proposed substantive and procedural legislative provisions to deal with both domestic and trans-national criminal activities. From this, several initiatives followed, in particular the proposal leading to the 2005 EU Framework Decision 2005/222/JHA on attacks against information systems[16]. The Framework Decision closely follows the definitional approach of the CoE convention and requires the EU Member States to criminalize intentional illegal access to information systems, illegal system interference (serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data) and illegal data interference. Such offences have to be punished by effective, proportionate and dissuasive criminal penalties; where an offence is committed in the context of a criminal organisation, causes substantial loss or affects essential interests, this must be considered an aggravating circumstance. To enhance cooperation, the Member States will exchange all relevant information; in particular, they must establish operational points of contact available twenty-four hours a day and seven days a week. Also other, more general, EU legislation covers aspects of the fight against cybercrime, such as the EU Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment[17], the EU

15 Document COM (2001) 890 final of 26.01.2001.

16 O. J. No. L 69 of 16.03.2005. p. 67.

17 O. J. No. L 149 of 02.06.2001, p. 1

Framework Decision 2004/68/JHA on sexual exploitation of children and child pornography[18] in relation to child pornography published using information systems or the EU Framework Decision 2008/913/JHA Decision on combating racism and xenophobia[19].

Institutional efforts of the EU include that cybercrime falls into the competence of the European Police Office (Europol) and the European Judicial Cooperation Unit (Eurojust). Furthermore, the EU has created a European Network and Information Security Agency (ENISA) in 2004[20] the main objective of which is to develop expertise, stimulate cooperation between the public and private sectors and provide assistance to the Commission and Member States in the field of network and information security (NIS).

Meanwhile, the EU has developed a complex approach to NIS. The 2006 communication "A Strategy for a Secure Information Society"[21] sets out a framework to carry forward and refine a coherent approach to NIS, among other priorities on fighting spam, spyware and malicious software. And on 22 May 2007, the European Commission presented a communication „Towards a general policy on the fight against cyber crime"[22] in 2007 which was welcomed by the Council of the EU on 8 November 2007[23]. The major objectives set out in the communication are

- to improve and facilitate coordination and cooperation between cybercrime units, other relevant authorities and experts, and
- to develop a coherent policy framework in the fight against cybercrime.

In more detail, cross-border operational cooperation shall be strengthened, the training of law enforcement officers shall be improved, and a broader public-private cooperation shall be achieved. The European Commission will also consider a legislative instrument on identity theft and take the initiative at raising awareness, especially among consumers, of the cost of and dangers posed by cybercrime. A particular focus is set on illegal content, and procedures to block and close down illegal internet sites shall be developed.

3. But given the global nature of cybercrime, even regional efforts such as undertaken in Europe will not suffice. Indeed, academics and research institutions have already developed valuable drafts of such an instrument (1.). There are also many decisions, resolutions and recommendations emanating from the United Nations (UN) on cybercrime and cyber security (2.). The most recent, most comprehensive and, in my eyes, most promising initiative, however, comes from the International Telecommunication Union (ITU) that has developed a "Global Cybersecurity Agenda" and recently published a "Global Strategic Report" which might well be a basic document for future UN negotiations on a "Global Convention against Cybercrime" (3.).

3.1. In 2001, the American Hoover Institution published a "Stanford Draft International Convention to Enhance Protection from Cyber Crime and Terrorism of 2000"[24] which is still the leading academic proposal for an international instrument against cybercrime. The Stanford Draft is designed to encourage universal recognition of basic offenses in cyberspace and universal agreement to cooperate in investigating, extraditing, and prosecuting perpetrators. Article 3 of the Draft describes the conduct it covers, including interfering with the function of a cyber system, cyber trespass, tampering with authentication systems, interfering with data, trafficking in illegal

18 O. J. No. L 13 of 20.01.2004, p. 44.

19 O. J. No. L 328 of 06.12.2008, p. 55.

20 Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency, O. J. No. L 77 of 13.03.2004, p. 1.

21 Document COM (2006) 251 final of 31.05.2006.

22 Document COM (2007) 267 final of 22.05.2007.

23 Document 14617/07 of 08.11.2007 p. 18-20.

24 Goodman/Sofaer (ed.), The Transnational Dimension of Cyber Crime and Terrorism, Hoover Institution Press, 2001, available at http://www.hoover.org/publications/books/3009861.html (visited March 2009).

cyber tools, using cyber systems to further terrorist offences and targeting critical infrastructures[25]. States Parties would agree to punish all the forms of conduct specified. Article 5 of the Draft confirms jurisdiction in States where offences are committed, offenders are citizens, reside or are present, or where the conduct of offenders has substantial effects, and establishes priority in jurisdiction (resting first where the offender is physically present when the offence occurs, second where substantial harm is suffered, and third in the State of the offender's dominant nationality). The Stanford Draft requires State Party cooperation through mutual legal assistance and law enforcement provisions. States Parties are obliged to exchange information, assist in gathering and preserving evidence, arrest alleged offenders, prosecute or extradite them, and to implement agreed international standards dealing with security and law enforcement. Article 12 of the Stanford Draft proposes an international Agency for Information Infrastructure Protection (AIIP). The AIIP is intended to serve as a formal structure in which interested groups will cooperate through experts in countries around the world in developing standards and practices concerning cyber security. All States Parties are represented in the AIIP Assembly, which would adopt objectives and policies consistent with the Convention, approve standards and practices for cooperation, and approve technical assistance programs, among other responsibilities. The AIIP Council, elected by the Assembly, would appoint committees to study particular problems and recommend measures to the Assembly. Article 13 of the Stanford Draft permits States Parties to set and maintain their own standards for privacy and human rights.

Not surprisingly, the Draft focuses on cyber terrorism defining it as the „use of a cyber system as a material factor in committing" a terrorist offence, and including acts „with a purpose of targeting the critical infrastructure of any State". Whereas such a wide concept of cyber terrorism may be questionable, the Stanford Draft proposes a convincing solution to the problem that cybercrime is a very dynamic phenomenon whereas traditional international conventions are more or less static and soon outdated: Under the Draft, the AIIP Council can propose, and the AIIP Assembly can adopt, implementing measures, modifications and supplementary agreements, including the addition of types of conduct to be considered criminal.

3.2. The UN has repeatedly dealt with computer crime, cybercrime and cyber security, in particular through the UN Office on Drugs and Crime (UNODC) and the UN Commission on Crime Prevention and Criminal Justice (CCPCJ), but also through General Assembly (GA) Resolutions. Relevant initiatives include (in chronological order):

- UNODC, Manual on the Prevention and Control of Computer-related Crime, 1994. While this publication is now in need of revision, it still serves as a reference.
- GA Resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on "Combating the Criminal Misuse of Information Technology" which invite Member States, when developing national law, policy and practice to combat the criminal misuse of information technologies, to take into account, inter alia, the work and achievements of the CCPCJ[26].
- GA Resolution 57/239 and 58/199 of 20 and 23 December 2002 on "Creation of a Global Culture of Cybersecurity" and "Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures" which invite Member States to take note of ongoing cybersecurity collaboration and to promote a culture of cybersecurity.
- Recommendations by the Workshop 6: "Measures to Combat Computer-Related Crime", held in Bangkok on 22 April 2005 as part of the Eleventh UN Congress on

25 Offences related to more controversial issues (including protection of intellectual property and regulation of political, ethical or religious content) were omitted in order to avoid lengthy and ideological discussions.

26 The CCPCJ is currently – inter alia – working on the criminal misuse and falsification of identity (identity-related crime) which is closely connected with internet and computer-related technology.

> Crime Prevention and Criminal Justice. The Bangkok Declaration on "Synergies and responses: Strategic Alliances in Crime Prevention and Criminal Justice" (endorsed by para. 2 of the GA Resolution 60/177 of 16 December 2005) called on Member States to further develop national measures and international cooperation against cybercrime and welcomed efforts to enhance cooperation to prevent, investigate and prosecute high-technology and computer-related crime (paras. 15, 16).

Given the variety and disparity of UN initiatives, a substantive analysis of UN policy against cybercrime is not easy. Anyway, there is a high level of political consciousness which constitutes a solid basis for an effort to consolidate the initiatives.

3.3. Insofar, an initiative recently taken by the International Telecommunication Union (ITU) might prove helpful and merits support, also by the International Association of Penal Law. The ITU and its Secretary General Touré appointed, in a meeting which took place in Geneva on 5 October 2007, a High Level Expert Group (HLEG) of about 60 members to whom belong experts from governments, industry, regional and international organisations, research and academic institutions from every part of the world. The HLEG is backed by the UN and sponsored by the President of Costa Rica and Nobel Peace Laureate Arias Sanchez who said at the meeting: „New and emerging threats to cyber security cannot be solved by any one nation alone. There is an urgent need for an international framework, giving us international principles and allowing rapid coordination between countries at the regional and global levels" (emphasis added). ITU's aim is to present a „Global Cybersecurity Agenda" (GCA) covering five areas: legal measures, technical and procedural measures, organisational structures, capacity building and international cooperation. Meanwhile, the HLEG has presented and published its "Global Strategic Report"[27] which is, in my view, for the time being not only the most recent but also one of the most relevant documents on cybercrime and cyber security. Concerning legal measures, the Global Strategic Report proposes the development of "model cybercrime legislation" compatible with existing national and regional legislation; the idea is to make such legislation binding by a UN instrument. The CoE's Convention on Cybercrime is recognized as "an example of legal measures realized as a regional initiative" but it is pointed that the convention is not a global instrument and should be supplemented taking into account modern developments and – among others – the problems of spam, identity theft, preparatory acts and massive and coordinated cyber-attacks against the operation of critical information infrastructure. Concerning international cooperation, the Global Strategic Report proposes to create a "focal point" within the ITU that works – among other issues – towards international harmonization in the various fields of cyber security. The Report also stresses the need for the monitoring, coordination and harmonization of international cooperation.

27 Available at http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/global_strategic_report.pdf (visited March 2009).