Preparatory Colloquium Section I

Section 1: Concept paper and questionnaire

Thomas Weigend

(A) Scope of questionnaire (see Annex 1 and Annex 2)

The questions in this Section generally deal with "cyber crime." This term is understood to cover criminal conduct that affects interests associated with the use of information and communication technology (ICT), such as the proper functioning of computer systems and the internet, the privacy and integrity of data stored or transferred in or through ICT, or the virtual identity of internet users. The common denominator and characteristic feature of all cyber crime offences and cyber crime investigation can be found in their relation to computer systems, computer networks and computer data on the one hand and to cyber systems, cyber networks and cyber data on the other hand. Cyber crime covers offenses concerning traditional computers as well as cloud cyber space and cyber databases.

National rapporteurs can contact the general rapporteur in case of further inquiries or questions: Prof. Dr. Thomas Weigend: thomas.weigend@uni-koeln.de

(B) Criminalisation

Please note that in this questionnaire only general characteristics of cyber crime offense definitions are of interest. Specific questions of individual crime definitions will be discussed in Section II of the Congress.

(1) Which specific legal interests are deemed to be in need of protection by criminal law (e.g., integrity of data processing systems, privacy of stored data)?
(2) Please give typical examples of criminal laws concerning
(a) attacks against IT systems
(b) violation of IT privacy
(c) forgery and manipulation of digitally stored data
(d) distribution of computer viruses
(e) crimes related to virtual identities of users, e.g., forging, stealing or damaging virtual personalities
(f) other innovative criminal prohibitions in the area of ICT and internet, e.g., criminalisation of the creation and possession of certain virtual images, violation of copyright in the virtual sphere.

(3) How is criminal conduct (actus reus) typically defined in these crimes (by description of act, by consequence, other)? How is the object defined ("data", "writings", contents)?
(4) Is criminal liability for certain cyber crime limited to particular groups of perpetrators and/or victims?
(5) Does criminal liability in the area of ICT and internet extend to merely reckless or negligent conduct?
(6) Are there specific differences between the definition of cyber crimes and "traditional" crimes?

(C) Legislative technique

(1) Are there specific problems with respect to the principle of legality (e.g., vagueness, open-ended reference of the crime definition to other regulations)?
(2) How does legislation avoid undue chilling effects on legitimate use of ICT or of the internet?
(3) How does criminal legislation avoid becoming obsolete in light of rapid technological innovation? E.g.,
- how are changes in the use of internet and social networks taken into account?
- how is the law adapted to technological progress (e.g., by reference to administrative regulations)?

(D) Extent of criminalisation

(1) To what extent do criminal laws cover mere preparatory acts that carry a risk of furthering abuse, e.g., acquisition or possession of software that can be used for "hacking", "phishing", computer fraud, or bypassing download protection? If so, has there been controversy about introducing such laws? Have legislatures made specific efforts to avoid over-criminalization?

(2) To what extent has the mere possession of certain data been criminalised? In what areas, and on what grounds? How is "possession" of data defined? Does the definition include temporary possession or mere viewing?
(3) To the extent that possession of or granting access to certain data have been defined as criminal, does criminal liability extend to service providers (e.g., hosting or access providers)? What are the requirements of their liability, especially concerning mens rea? Are providers obliged to monitor and control what information they provide or offer access to? Are providers obliged to provide information on the identity of users? Are providers obliged to prevent access to certain information? If so, under what conditions, and at whose cost? Is there criminal liability for violating such obligations?
(4) What general, in particular constitutional limits to criminalising conduct have been discussed with respect to ICT and internet crime (e.g., freedom of speech, freedom of the press, freedom of association, privacy, "harm principle", requirement of an act, mens rea requirements)?
(5) Does the law provide for criminal sanctions specifically targeting cyber criminals, (e.g., a temporary ban from using the internet)?

(E) Alternatives to Criminalisation

(1) What role does criminal law play in relation to other ways of combatting abuse of ICT and the internet? What is the relationship of civil and administrative sanctions (payment of damages, closing of enterprise, etc.) to criminal sanctions in the area of ICT?
(2) What non-criminal means of combatting offensive websites are used/propagated (e.g., closing down websites, blocking access to websites)?
(3) To what extent are ICT users expected to protect themselves (e.g., by encryption of messages, using passwords, using protective software)? Are there sanctions for not protecting one's computer to a reasonable extent, e.g., by using anti-virus software or protecting access to private networks by password? Does the lack of reasonable self-protection provide a defense for defendants accused of illegally entering or abusing another person's network or abusing their data?

(F) Limiting anonymity

(1) Are there laws or regulations obliging internet service providers to store users' personal data, including history of internet use? Can providers be obliged to provide such data to law enforcement agencies?
(2) Are there laws or regulations obliging an internet service provider to register users prior to providing services?
(3) Are there laws or regulations limiting the encryption of files and messages on the internet? Can suspects be forced to disclose passwords they use?

(G) Internationalisation

(1) Does domestic law apply to data entered into the internet abroad? Is there a requirement of "double criminality" with respect to entering data from abroad?
(2) To what extent has your country's criminal law in the area of ICT and internet been influenced by international legal instruments?
(3) Does your country participate in discussions about the harmonisation of cybercrime legislation (such as the U.N. intergovernmental expert group on cybercrime)?

(H) Future developments

Please indicate current trends of legislation and legal debate in your country concerning ICT and internet crime.

Annex 1

John A.E. Vervaele

(1) Definition of Information Society? Substantive elements of a definition

No one single information society concept is predominant. Scientists are struggling about definitions and values of the concept and focus on economic, technical, sociological and cultural patterns. Post modern society often is characterized as an "information society", because of the widely spread availability and usage of Information and Communication Technology (ICT). The most common definition of information society lays indeed emphasis on technological innovation. Information processing, storage and transmission have led to the application of information and communication technology (ICT), and related biotechnology and nanotechnology, in virtually all corners of society. The information society is a postindustrial society in which information and knowledge are key-resources and are playing a pivotal role (Bell, 1973 & 1979).

But, information societies are not solely defined by the technological infrastructure in place, but rather as multidimensional phenomena. Bates (1984) pointed out that any information society is a complex web not only of technological infrastructure, but also an economic structure, a pattern of social relations, organizational patterns, and other facets of social organization. So, it is important not to focus only on the technological side, but also on the social attributes of the information society, including the social impact of the information revolution on social organizations, including the criminal justice system.

Moreover, the post modern age of information technology transforms the content, accessibility and utilization of information and knowledge in the social organizations, including the criminal justice system. The relationship between knowledge and order has fundamentally changed. The transformation of communications into instantaneous information-making technology has changed the way society values knowledge. In this rapidly changing age, the structure of traditional authority is being undermined and replaced by an alternative method of societal control. The emergence of a new technological paradigm based on ICT has resulted in a network society Castells1996), in which the key social structures and activities are organized around electronically processed information networks. There is an even deeper transformation of political institutions in the network society: the rise of a new form of state (network state) that gradually replaces the nation-states of the industrial era. In this rapidly changing age, the structure of traditional authority is being undermined and replaced by an alternative method of societal control (surveillance society). The transition from the nation-state to the network state is an organizational and political process prompted by the transformation of political management, representation and domination in the conditions of the network society. All these transformations require the diffusion of interactive, multilayered networking as the organizational form of the public sector.

Information and knowledge are key-resources of the information society, affecting the social and political structure of society and state and affecting the function, structure and content of the criminal justice system.

(2) The interrelatedness of the questionnaires for all four sections

First of all we should use a common working definition. It is clear that computer crime is too narrow for our topic and that "information criminal law or offences related to the information society" is not a well established concept either.

For this reasons we have to use a common definition and a limited focus.

As for as the definition is concerned I do propose to use the concept cyber crime, but with a definition that includes a wide variety of new phenomena and developments.

The common denominator and characteristics features of all cybercrime offences and cybercrime investigation can be found in their relationship to computer systems-computer networks-computer data at the one hand but also to cyber systems-cyber networks-cyber data at the other hand. It goes from the classic computers to the use of the cloud cyber space and cyber databases,

Second, as this is a very broad area, we should focus on the most interesting new areas where our resolutions could produce added value. The outcome of the discussions with the four general rapporteurs is that we will focus on the following legal interests in the field of cybercrime:

1. The integrity and functionality of the cyber-ICT system (CIA offences)

2. Protection of privacy
3. Protection of digital personality
4. Protection against illegal content
5. Protection of property (including intellectual property rights)
6. Protection against acts committed exclusively in the virtual world
7. Protection of enforcement system (non-compliance offences)

(3) References

Daniel Bell, The Coming of Post-Industrial Society, New York, Basic Books , 1976.

Manuel Castells, The Rise of the Network Society. The Information Age: Economy, Society and Culture Volume 1. Malden: Blackwell. 2d Edition, 2000

S. Sassen, The global city , New York-London, Princeton University Press, 2d edition, 2001.

U.Sieber, Mastering Complexity in the Global Cyberspace, in M. Delmas-Marty & M Pieth. Les chemins de l'harmonisation Pénale, Paris 2008, 127-202.

Annex 2

General considerations

Thomas Weigend

(1) Information technology in need of protection

To an extent that was hardly foreseeable even 30 years ago, social life on a worldwide scale depends on the proper functioning of information and communication technology (ICT) and the internet. This dependence extends to both the public and the private spheres. On an individual level, interpersonal communication, but also large parts of leisure activity including information-gathering are ICT-based, and many individuals have heavily invested in the development and maintenance of their digital personality (or personalities), e.g. in personal websites and blogs or communication services such as Facebook and Twitter.

These developments have led to a situation where attacks on the integrity of ICT have become serious threats that can affect not only individual interests but also the security of states, important business interests, and the economic system as a whole. Hacking and data falsification, violations of the privacy of digitally transmitted communications, and "identity theft" on the internet are threatening the well-being not only of individuals but also of business firms and states.

(2) Information technology and the worldwide web as a means to commit crime

ICT also has transformed the quantitative dimension of certain assaults on legally protected interests. Whereas in earlier times persons with criminal intentions to defraud or to spread libellous information had to approach each potential recipient of information individually, it is now possible to spread information to hundreds of thousands of persons within a second by using automated e-mail services or websites. The use of computer viruses to create bot networks can further multiply the effectiveness of an assault and involve up to a million of computers belonging to persons who are unaware of the fact that their addresses are being misused. The existence of a worldwide web and the possibilities of computer technology thus enable persons with criminal intentions to cause maximal harm with minimal effort.

Other features of ICT further contribute to the attractiveness of the net for criminal assaults on individual or collective interests. The possibility of acting anonymously and of using a false identity enables criminals to remain undetected. Detection is further complicated by the extremely high speed of data transfer coupled with routine deletion of transfer data by service providers. The origins of the worldwide web as a device for the quick transfer of secret military information further contribute to the shielding of network users from detection: the worldwide web was purposely devised as a network with many overlapping and independent lines of communication, thus making the web resistent to any attempt of disturbing its functioning through external intervention. The web structure also makes it highly difficult to trace individual items of information back to one source or to effectively block access to an information.

(3) The Role of the Criminal Law

(a) Protecting ICT against Crime

The special sensitivity of ICT to criminal attacks, and the great harm that can be caused by such attacks, make it necessary to employ the criminal law in preventing and sanctioning acts that interfere with the integrity of communications based on ICT. Many legal systems have enacted criminal provisions dealing with such phenomena as data theft, data falsification, and invading protected data bases. Due to the inherently transnational character of the worldwide web, international organisations have attempted to harmonize national legislation in this area (see, e.g., the Cybercrime Convention drafted by the Council of Europe).

Many of the general problems of criminalization (precisely defining the criminal act, avoiding overreach and chilling effects on legitimate conduct, keeping up with technological progress) pose themselves in this area, and some of them are especially acute when a legislature sets out to incriminate assaults on the integrity of IT. The following specific problems come to mind:

(i) Does the progress of ICT lead to new legal interests, and how can they be defined and protected? For example, is there a need to protect "virtual identities" against theft or forgery, and if so, how can that goal be accomplished?
(ii) How can criminal law keep up with the quick pace of development of information technology and the character and contents of the worldwide web?

(iii) Given the sophisticated and ever-changing character of the interests to be protected, how can criminal laws be sufficiently precise to satisfy the principle of legality and yet avoid glaring loopholes? How can criminal "acts" be defined when all that can be noticed are certain effects whereas the "act" is committed by an automated computer system?
(iv) What role can or should incrimination of conduct play in relation to other means of protecting sensitive ICT interests? According to the ultima ratio principle, criminal law should not be employed as the primary means for preserving the integrity of ICT systems. Should criminal laws, for example, apply in addition to effective civil sanctions, e.g., payment of damages for copyright violations? ICT itself provides efficient devices (e.g., encryption, anti-virus and anti-hacking programs, protection against unauthorized download of copyrighted materials) for defending against attacks. This leads to the question whether criminal law should apply only where such devices cannot provide sufficient protection. But one might also think of obliging users by law to install protective programs, and of creating criminal liability for any failure to reasonably protect one's computer against virus infection (because careless users help to spread viruses).
(v) Many legal systems do not generally regard as punishable activity that is merely in preparation of harmful behavior. In the context of ICT criminality, however, the impending harm that can be so grave that certain preparatory measures may be criminalized. For example, some legal systems have criminal provisions against offering or selling (or even possessing?) software especially designed for the commission of internet crime, e.g., for "cracking" passwords or for bypassing download protection. In consonance with the Council of Europe's Cybercrime Convention, some states have also criminalized the sale or purchase of software designed to facilitate the commission of computer fraud. The limits of the legitimate extension of ICT criminality still need to be discussed.

(b) Protecting against Crime Committed through ICT

As has been mentioned above, ICT has created a whole new world of opportunities for individuals intending to commit criminal offenses. Criminal legislation may seek to adapt to this development by using specific tools for controlling and sanctioning the abuse of ICT and especially the internet for committing "ordinary" offenses. Since the focus of the questionnaire is not on these legislative measures, they will be mentioned here only briefly.

(i) Limiting anonymity

One aspect of the internet that offers opportunities for crime is the protection of anonymity that the web provides. Several measures have been suggested to limit anonymity, so as to enhance the chance of detection and identification of offenders. One (controversial) measure imposed by the European Union is an obligation on access providers to store transfer data for several months in order to make it possible to retrace data transfers back to the computer of origin. Other measures under discussion include limits on the complexity of encryptions and an obligation of computer owners to divulge passwords. Such measures may appear defensible in the context of an ongoing investigation for serious crime, but they necessarily spill over to instances of permissible use of the internet and have the potential of strongly reducing the attractiveness (and thus the profitability) of the net as well as of violating users' legitimate privacy interests.

(ii) Controlling content

There is an understandable tendency of legal systems to extend existing criminal prohibitions with regard to written or printed materials (e.g., pornography, incitement to religious or racial hatred, instruction to commit crimes, disclosure of protected state, military or business secrets) to similar materials distributed by means of ICT. This tendency raises a number of specific problems: first, the transnational character of the worldwide web makes it difficult to enforce national standards, and international agreement on the proper scope of restrictions of speech is difficult to achieve. Second, the ultima ratio principle raises the issue whether measures short of the imposition of criminal sanctions are at least equally effective. Third, the anonymity of the net leads to the question whether it is possible to extend criminal responsibility for illegal contents to (easily identifiable) providers of internet services, which might reduce the difficulty of piercing the shield of anonymity when attempting to effectively control internet content.

The difference of national interests and standards in prohibiting (or protecting) speech seems to be difficult to overcome (this is an aspect to be treated mainly in Section IV of the Congress) Legal system differ strongly as to (i) what content they regard as harmful or dangerous and (ii) where they draw the line between materials protected by freedom of speech and materials the proliferation or even possession of which will be criminally prosecuted. Beyond the technical issue of the applicability of national criminal laws to materials available on the internet (but presumably "posted" by foreign citizens in foreign countries), these differences create a great impediment to international cooperation in the prosecution of (possible) content offenses. International conventions in this area might resolve that problem, but their drawback is that they tend to maximize criminalisation, because each participating country adds its "pet crimes" to the list of prohibited conduct and there is little political support for retaining breathing space for individual freedom of expression.

Alternatives to criminal prosecution for offensive content are blocking of access to (through the use of software) and deletion of undesirable websites. However, even if access blocking is technically possible it requires cooperation of all nations to be effective, because a block installed by one national agency can easily be circumvented by using an access provided by a foreign firm that does not cooperate with the national agency in question. Deletion, if possible, might be likewise of limited effect because an offending webpage can easily (even automatically) be restored under a different name.

This leads to the issue of making access and/or service providers criminally responsible for maintaining and keeping accessible illegal content. Under this approach, providers would be obliged to "police" and if necessary censor the net. Content providers could be required to either react to complaints about illegal content or even to proactively investigate the contents they provide for prohibited materials. Even if that were technically possible, the normative question arises on what legal basis a (costly) duty to police the net could be imposed on content providers. If one postulates an affirmative legal duty for providers, their criminal liability for breaching this duty could be based on the doctrines of accessorial liability or omission. In that regard, provider liability is to be discussed in Section I on the General Part.