Section 4: Concept paper and questionnaire

André Klip

(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. André Klip: andre.klip@maastrichtuniversity.nl

(B) Jurisdictional issues

(1)(a) How does your country locate the place of the commission of a crime in cyberspace?
(b) Does your national law consider it necessary and possible to locate the place where information and evidence is held? Where is the information that one can find on the web? Is it where the computer of the user is physically present? Is it there where the provider of the network has its (legal or factual) seat? Which provider? Or is it the place where the individual who made the data available? If these questions are not considered to be legally relevant, please state why.
(2) Can cyber crime do without a determination of the locus delicti in your criminal justice system? Why (not)?
(3) Which jurisdictional rules apply to cyber crime like hate speech via internet, hacking, attacks on computer systems etc? If your state does not have jurisdiction over such offences, is that considered to be problematic?
(4) Does your national law provide rules on the prevention or settlement of conflicts of jurisdiction? Is there any practice on it?
(5) Can cyber crime do without jurisdictional principles in your criminal justice system, which would in essence mean that national criminal law is applicable universally? Should this be limited to certain crimes, or be conditional on the basis of a treaty?

(C) Substantive criminal law and sanctions

Which cyber crime offences under your national criminal justice system do you consider to have a transnational dimension?
To what extent do definitions of cyber crime offences contain jurisdictional elements?
To what extent do general part rules on commission, conspiracy or any other form of participation contain jurisdictional elements?
Do you consider cyber crime offences a matter that a state can regulate on its own? If so, please state how a state may do that. If not, please state why it cannot do that.
Does your national criminal provide for criminal responsibility for (international) corporations/ providers? Does the attribution of responsibility have any jurisdictional implications?

(D) Cooperation in criminal matters

To what extent do specificities of information technology change the nature of mutual assistance?
(2)(a) Does your country provide for the interception of (wireless) telecommunication? Under which conditions?
(b) To what extent is it relevant that a provider or a satellite may be located outside the borders of the country?
(c) Does your national law provide for mutual legal assistance concerning interception of telecommunication? Did your country conclude international conventions on it?
(3) To what extent do general grounds for refusal apply concerning internet searches and other means to look into computers and networks located elsewhere?
(4) Is in your national law the double criminality requirement for cooperation justified in situations in which the perpetrator caused effects from a state in which the conduct was allowed into a state where the conduct is criminalised?
(5) Does your national law allow for extraterritorial investigations? Under which conditions? Please answer both for the situation that your national law enforcement authorities need information as when foreign authorities need information available in your state.

(6) Is *self service* (obtaining evidence in another state without asking permission) permitted? What conditions should be fulfilled in order to allow self service? Please differentiate for public and protected information. What is the (both active and passive) practice in your country?
(7) If so, does this legislation also apply to searches to be performed on the publicly accessible web, or in computers located outside the country?
(8) Is your country a party to Passenger Name Record (PNR) (financial transactions, DNA-exchange, visa matters or similar) agreements? Please specify and state how the exchange of data is implemented into national law. Does your country have an on call unit that is staffed on a 24/7 basis to exchange data? Limit yourself to the issues relevant for the use of information for criminal investigation.
(9) To what extent will data referred to in your answer to the previous question be exchanged for criminal investigation and on which legal basis? To what extent does the person involved have the possibility to prevent/ correct/ delete information? To what extent can this information be used as evidence? Does the law of your country allow for a Notice and Take-Down of a website containing illegal information? Is there a practice? Does the seat of the provider, owner of the site or any other foreign element play a role?
(10) Do you think an international enforcement system to implement decisions (e.g. internet banning orders or disqualifications) in the area of cyber crime is possible? Why (not)?
(11) Does your country allow for direct consultation of national or international databases containing information relevant for criminal investigations (without a request)?
(12) Does your state participate in Interpol/ Europol/ Eurojust or any other supranational office dealing with the exchange of information? Under which conditions?

(E) Human rights concerns

Which human rights or constitutional norms are applicable in the context of criminal investigations using information technology? Is it for the determination of the applicable human rights rules relevant where the investigations are considered to have been conducted? How is the responsibility or accountability of your state involved in international cooperation regulated? Is your state for instance accountable for the use of information collected by another state in violation of international human rights standards?

(F) Future developments

Modern telecommunication creates the possibility of contacting accused, victims and witnesses directly over the border. Should this be allowed, and if so, under which conditions? If not, should the classical rules on mutual assistance be applied (request and answer) and why?
Is there any legal impediment under the law of your country to court hearings via the screen (skype or other means) in transnational cases? If so which? If not, is there any practice?
Is there any other issue related to Information society and international criminal law which currently plays a role in your country and has not been brought up in all the questions before?

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

Concept paper

André Klip

(1) Introduction

The fact that modern society has changed into an information society may have dramatic consequences for various aspects of international criminal law. This justifies renewed attention within our association. It is not the first time that the AIDP looked into the topic, albeit quite some years ago, and things have changed.[1] Among other things, the globalisation of our society means that human behaviour may have its effect at many more locations than the place where the initiator of the conduct acted. Google earth, Street View, and Facebook and Hyves make clear to us that for many there is little that others may not be able to see. Big Brother is watching us, what are the implications for international criminal law? Cloud computing raises the question of where data are stored and which legislation applies to it.[2]

In the context of criminal law these extraterritorial effects of conduct may result from the use of certain technologies, such as telecommunication, computers and the web. Hackers may enter a network or an individual computer located in one state from a computer located at the other side of the world. Hate speech may be uttered through twitter, email messages or you tube tapes and have a global expansion. With regard to the material conduct various issues concerning jurisdiction over the conduct and its locus arise.

With regard to the investigations into crimes committed in modern times, the information society leads to new situations and raises new questions. The investigation into an international network for the production of child pornography and the dissemination of its products may require to visit websites, to enter their protected areas, to look into mail boxes, discussion and news groups and to identify the individual IP-addresses of computers.

Also wireless means of communication poses new problems to the law enforcement agencies, because the transmission of data may involve various states or international organisations. The person using a cell phone in one state may converse with a person in another state. However, the satellite(s) transmitting the conversation may be located in other states or in space. What does this mean for the possibilities of intercepting the conversation?

In times in which there are various situations in which it is important to have a certain position of information that will enable the state to prevent or respond to terrorist attacks, states have concluded so called Passenger Name Record agreements. In addition, states have developed (common) databases that may be consulted directly without intervention of the state that supplied the information. For instance, within some states of the European Union, the DNA-database provides for direct consultation whether a new sample matches DNA-profiles already present in the national database and that of the “cooperating” state.

Thus far, despite its presence for quite some decades already, the emergence of cyber crime did not lead to much legislative activity on the international level. The main documents are the Convention on Cybercrime,[3] and its Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.[4] The drafters of the Convention on Cybercrime did relate the necessity of the convention to developments in the society as a whole.[5] What other instruments exist on an international, regional or national level? Despite the fact that states may legislate, technological steps may make the role of private parties increasingly important.

---

[1] See the general report by Cole Durham, The Emerging Structures of Criminal Information Law: Tracing the Contours of a New Paradigm, 64 RIDP 1993, p. 79-117.

[2] See Laviero Buono, the Global Challenge of Cloud Computing and EU Law, Eucrim 2010, p. 117-124.

[3] Budapest, 23 november 2001, ETS 185, as of 8 November 2010 30 ratifications.

[4] Strasbourg, 28 January 2003, ETS 189, as of 8 November 2010 18 ratifications.

[5] In the preamble to the Convention on Cybercrime the necessity of international legislation in a global information society has been described with the following arguments: “Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia,* by adopting appropriate legislation and fostering international co-operation; Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks; Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks; Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies; Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters.”

(2) Focus on international aspects

As a thumb rule, relevant for the National Rapporteurs of section 4, it is important that the focus will always be on the international aspects of each segment of their national law. For instance, when rules applicable to the collection and value of evidence are identified, for section 4 it is more important to know how it is determined which state can apply its legislation on it, than to characterise the nature of this evidence in the evidentiary context of the national criminal justice system. The focus of the National Report will always be on the description of the national legal situation in an international context.

(3) Questions related to jurisdiction over crimes and the locus of the crimes

With the growing importance of the technical developments old legal concepts may have difficulties to keep pace. Whereas in the past it was relatively easy to locate conduct to a specific location (locus delicti), it increasingly becomes difficult to locate conduct in cyberspace. States generally have a tendency to prevent negative conflicts of jurisdiction and have increasingly extended the scope of application of their criminal law. They intended to solve the problem by widening jurisdictional principles. Additionally, the cross-border nature of the offence as such has increased multiple jurisdiction.

As a consequence of the practice of widening the extraterritorial application of criminal law, positive conflicts exist by definition. Numerous questions can be raised as a result of it. Should this be prevented? Is this problematic? Does this lead to real problems in practice, or is it in essence an academic problem?[6]

The fact that if all states extend their jurisdiction, automatically concurrent jurisdiction comes into being, raises the question whether certain crimes, for which it may be difficult to find the locus delicti, could do without a locus. A key question is thus whether modern crimes can do without jurisdictional principles, which would in essence mean that national criminal law is applicable universally. Is this a road to follow? Should this be limited to certain crimes, for instance crimes, for which there is a conventional basis to criminalise and vest extraterritorial jurisdiction over it,[7] or should this be allowed for all crimes? In the latter situation, national criminal is applicable all over the world, which does seem to be an attractive situation. Could that be solved by allowing for prosecution in cases of a relevant nexus only? To what extent does the concurrent jurisdiction in practice lead to inertion? Does it lead to a *bystander effect*, in which states do not investigate or prosecute crimes committed outside the country, because there are many other states that may have jurisdiction over the offence?

Another way to approach things could be that for certain crimes, for which the locus delicti is difficult to find or does imply concurrent jurisdiction, supranational adjudication should be provided. The advantage would be of course that a supranational tribunal would have the power to solve the jurisdictional conflict in a manner binding to the states involved. Additionally, a more specialised tribunal and prosecution could deal with specific forms of transnational crime, which go far beyond the possibilities of national law enforcement authorities. How would an international responsibility for corporations actually work? However, it also means that a further international tribunal might be established, leading to further segregation of the enforcement of the law.

Added to the difficulties in locating the crime is the requirement of double criminality. Most jurisdictional principles, apart from the universality principle, do require that the conduct most also be criminalised according to the law of the place where it was committed. Given the developments of the information society, it is relevant to raise the question whether this requirement still serves a purpose. What is the justification for maintaining a double criminality requirement in the context of the information society of today and for the coming decades? Could we do without it? Which issues are at stake if the rule would be abolished? Could the interests protected by the double criminality rule be safeguarded in other manners?

(4) Questions related to investigations

Thus far, the rules on the collection of evidence outside the territory have been very straightforward and clear. If law enforcement agencies need information and evidence from elsewhere, they must request foreign authorities to produce it. Police officers of one state may not go without permission to the territory of another state to get what they need. The circumstances currently are

[6] In a recent comparative study commissioned by the Netherlands' Ministry of Justice, Klip and Massa conclude that there are hardly any prosecutions for crimes with a locus delicti outside a state's territory. See André Klip and Anne-Sophie Massa, Communicerende grondslagen voor extraterritoriale rechtsmacht, Maastricht University 2010 http://www.wodc.nl/onderzoeksdatabase/vestiging-rechtsmacht.aspx?cp=44&cs=6802

[7] Such as, e.g. the Convention on Cybercrime.

somewhat different than in the past, because telecommunication networks may enable law enforcement agencies to obtain information and evidence without leaving their own country. A preliminary question is whether it is necessary and possible to locate the place where information and evidence is held? Where is the information that one can find on the web? Is it where the computer of the user is physically present? Is it there where the provider of the network has its (legal or factual) seat? Which provider? Or is it the place where the individual who made the data available?

In the context of the information society and obtaining information and evidence for purposes of criminal investigation various situations deserve attention, presumed it is still possible to locate information and evidence: 1. Open information and evidence. This is information which is publicly accessible simply by surfing through the net.
2. Protected information. Information which cannot be publicly accessed, but which may be accessed by hacking. 3. Information and evidence that require to take over a computer or network located in another country.

States continue to have rather strict rules prohibiting the physical presence of foreign law enforcement agents on their territory.[8] Do these rules still apply in the context of modern crimes? Do these rules also apply when law enforcement agents do not physically enter the territory of another state, but do search in networks or computers located in another state. Do the same rules apply and if so, how do they apply? If the rules prohibiting physical presence do not apply, why is that so?

The consequences of not applying the regular rules on mutual assistance in criminal matters are more than symbolic. It would lead to a situation in which assistance from another country is no longer requested and given, but simply obtained through *self service*. This would result in a situation in which traditional grounds for refusal (double criminality, nature of the crime, double jeopardy etc) could no longer be applied. Would it be possible or necessary to reduce the application of grounds for refusal in this area? What are the (theoretical/ practical) consequences of accepting self service as one of the modalities for international assistance in criminal matters?

Once again, it seems that technical possibilities may determine the legal developments and possibilities. This phenomenon may lead to highly interesting theoretical questions about where the primacy for the development of the law should be. However, there are also questions of a more practical legal nature. An example of that relates to the interception of wireless telecommunication. If two persons converse by making use of cell phones, it may involve six states.[9] Should all these states have a say in whether conversations may be intercepted? Or should this be limited to the state that wishes to intercept and why (not)?

Some states and international organisations possess satellites or other devices that enable them to have a clear and detailed picture of every place in the world. Should the law regulate the use for purposes of criminal investigation and prosecution? If so, on which level should this be regulated, national or international and what are the issues at stake?[10]

(5) Questions related to classical mutual assistance in criminal matters

To what extent does the information society change the nature of classical mutual assistance?[11] Although some forms of self service may come up and may even be legally accepted, it is unlikely that international mutual legal assistance in criminal matters will completely disappear with the further development of the information society.

The very fact that it has become increasingly simple to speak with persons abroad through audio-visual techniques (skype, videoconference) raises the question whether this should not lead to a higher threshold for extradition for the purposes of prosecution. If the accused is not present in the state that prosecutes him extradition is likely to take place. In light of the serious infringement on the liberty of the accused, the question may be raised whether it should be preferred to conduct the trial via a video-link. Also the presumption of innocence would oppose burdensome extradition. Should we reserve extradition for convicted persons? Do we envisage a virtual court room, in which hearings may take place, whilst nobody is present in the real court room?

Similarly, modern telecommunication creates the possibility of contacting accused, victims and witnesses directly. Should this be allowed, and if so, under which conditions? If not, should the classical rules on mutual assistance be applied (request and answer)

[8] Police officers may only enter another country and perform their duties if this finds a basis in a codified international agreement or on the basis of ad hoc permission. The use of coercive measures is generally ruled out. With minor exceptions, such as the apprehension of a fugitive in the case of a cross border hot pursuit. See, e.g. Article 41 of the Convention Implementing the Schengen Agreement.
[9] Gert Vermeulen, Wederzijdse rechtshulp in strafzaken in de Europese Unie, dissertation Gent 1999, p. 224-293.
[10] It reminds us of the "telescreens" predicted by George Orwell in his famous novel 1984.
[11] It is interesting to see that the Convention on Cybercrime completely follows the classical principles of international cooperation in criminal matters: a request send by one state to another to render assistance.

and why? The very fact that a lot of information is freely accessible anyway and that in many cases persons involved have submitted the information voluntarily, raises the question why states should still have the power to control whether assistance will be given or not. On the other hand, the view on whether a certain act is within the realm of freedom of speech or a serious crime of breaking confidentiality may differ. Imagine, the US wants certain information in order to investigate the fact that numerous secret and restricted documents concerning the Iraq war have been made available through wikileaks.

What about obligations to retain data on information transmission? Do providers have the obligation to organise their network in such a manner that they may comply with all different and complicated request for assistance from law enforcement agencies of other states? How could this be done with providers not having a seat in the relevant state? Also of a more general nature is, apart from the relevant legislation, the question whether states do have the know-how to deal with crimes committed in the information society. Do law enforcement agencies have the expertise to effectively investigate and enforce the offences in cyberspace?

(6) Questions related to obtaining an information position[12]

Especially as part of a package of measures related to combating terrorism states are eager to obtain a good information position in order to prevent terrorist attacks or other crimes from taking place. Given the use of air traffic in the past, as a means of terrorist attacks, states have given priority to have more knowledge on passengers and on freight. Regarding passengers, so called Passenger Name Records agreements have been concluded.[13] Also in other areas, such as financial transactions and visa matters, data are exchanged.

We must be aware of the fact that we are entering here the sphere of privacy law. Whereas on the hand, it should be prevented that the focus of our discussions should be on the elements of the protection of privacy, it is, on the other hand, inevitable that some elements of privacy law will be discussed. National Rapporteurs are requested to focus on the use made for criminal investigations of data submitted or exchanged under PNR (financial transactions or any other) agreements for criminal investigation, not for other purposes such as immigration policy or data retention rules in general. To what extent will the data be exchanged for criminal investigation and on which legal basis? To what extent does the person involved have the possibility to prevent/ correct/ delete information? To what extent can exchanged information be used as evidence?[14]

A further recent development is the establishment of supranational databases and the online consulting of each other's databases. An example of that relates to the EU, in which some Member States have established a mechanism to retrieve data on DNA, licence numbers of vehicles and finger prints directly from another Member State.[15] One of the consequences is, that the state whose data is used, no longer is requested to give information and does not take a decision in individual cases to do so. It also means that grounds for refusal are no longer considered and applied in the initial stage of information exchange.[16] Is this a good development? Within the EU further plans have been developed to create direct access to the criminal records of all Member States.[17] Is that a good thing? Can similar developments be identified in other regions of the world?

---

[12] It is referred to the definition given by Hans Nijboer, General Rapporteur to Section III: "The existence and the use of enormous amounts of operational information is sometimes referred to as the *information position* of investigative and prosecutorial authorities.

[13] The EU concluded agreements with the United States and with Australia on this matter. See http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/431&format=HTML&aged=0&language=EN&guiLanguage=en
Council Decision 2010/16/CFSP/JHA of 30 November 2009 on the signing, on behalf of the European Union, of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program, OJ 2010, L 8/11.

[14] In the EU context, a special legal instrument has been adopted regulating the data protection rules in international cooperation in criminal matters. See Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ 2008, L 350/60.

[15] Council Decision 2009/1023 of 21 September 2009 on the signing, on behalf of the European Union, and on the provisional application of certain provisions of the Agreement between the European Union and Iceland and Norway on the application of certain provisions of Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime and Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, and the Annex thereto, OJ 2009, L 353/1; Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ 2008, L 210/1.

[16] However, the relevant legal instruments stipulate that if the information is to be used as evidence, a regular request for international assistance must follow.

[17] Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, OJ 2009, L 93/23.

(7) Questions related to direct enforcement

The almost unlimited possibilities of information technology do raise questions with regard to whether states may directly enforce judgments, notifications, provisional measures etc by making use of information technology, without asking permission of whatever other state.

In a situation in which there is a legal decision that a certain website must close down, because it contains child pornography, hate speech or other illegal material, should it be allowed for law enforcement agencies to hack that site in order to prevent it from further committing crimes?

The notification of judgements, decisions, summons and other legal documents may have legal consequences. Should the law attach these consequences also to notifications send by information technology?[18] Similarly, should states have the competence to impose upon banks and other financial institutions to confiscate certain financial means in order to keep this for purposes of confiscation of proceeds from crime?

(8) Concluding remarks

In sum, at first sight, it seems that the impact of the information society to international criminal law is threefold. The first is that the information society creates a transnational threat for certain legal goods, whilst other may remain unaffected by it. The second is that the information society creates, on the other hand, a tool for criminal justice. The third major impact relates to sovereignty. What does sovereignty mean in our age? Traditionally, the concept of sovereignty gives states a monopoly on the application of criminal law and criminal procedure, based on the territoriality principle. The information society has seriously decreased (or maybe even taken away) the value and importance of territoriality. What does this mean for sovereignty? In sum, the focus of this section is on the extraterritoriality of the conduct, the extraterritoriality of the investigation and the extraterritoriality of the enforcement.

[18] In 2010, e.g., the German postal services introduced the electronic Zustellung, equal to a formal notification by an usher.