Project on Cybercrime
www.coe.int/cybercrime

Economic Crime Division
Directorate General of
Human Rights and Legal Affairs
Strasbourg, France

Version 5 March 2009

Discussion paper (draft)

Cybercrime and Internet jurisdiction

prepared by
Prof. Dr. Henrik W.K.Kaspersen
Vrije Universiteit Amsterdam
The Netherlands

This report has been prepared within the framework of the Project on Cybercrime of the Council of Europe.

Contact

For further information please contact:

Economic Crime Division
Directorate General of Human Rights and Legal Affairs
Council of Europe
Strasbourg, France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int

Content

1 Introduction

1. This report has been commissioned by the Project on Cybercrime of the Council of Europe. It is meant to provide an inventory of possible problems and to study solutions concerning jurisdiction issues related to cyber crime. It was left to the discretion of the author to determine the scope, structure and content of the report and to include issues as they appeared useful for further discussion.

2. It took little time to choose 'Internet jurisdiction' as an appealing title for this report. However, it took more time to determine the precise scope and content of this paper and even considerably more time and energy to decide on the message that this paper should convey to its readers. In relation to that a title has been chosen that is neutral enough to cover the content and conclusions of this report. It was not my aim to provide a comprehensive analytic summary of internet criminal jurisdiction aspects in theory and praxis. A study on jurisdiction may deal with the issue from a point of public international law. It may also consider how and to what extent domestic law of States and the courts of a State apply this principles. The latter does not belong to the scope of this report. Decisions of domestic courts therefore will not be discussed. The main purpose is to examine what the consequences are of the application of the jurisdiction principles in relation to Cybercrime and if that would require international measures or regulation.

3. This was the usual approach in literature, where the emergence of a cyber crime with it specific characteristics and borderless structure would urge to develop new and additional jurisdiction principles and arrangements under international public to accommodate the virtual world and its global population. Implicitly, this assumes that the virtual world is a separate space, room, sphere etc. that can be fully isolated from the real world in which legal subjects have intercourse with other legal subjects and where the legal order should consist of different rules, dedicated to the electronic, most of the time cross-border mutually interaction between internet users. In the nineties, it was therefore referred to the *hype* notion *electronic highway* or *cyber space*. Indeed, the internet has proven itself as an indispensable facility in our modern and global society. It is generally accepted that ICT and the internet caused an important shift of paradigms that forced legislators and the legal profession to reconsider the definition, detailing and interpretation of certain domains of law. This report recognises that the electronic world brought considerable changes, but will not consider cyber space in splendid isolation: it is part of our real world and it should be looked at it as such. It means that use should me made of the legal concepts that have been developed in past centuries, even if adaptations to the electronic environment are required.

4. At the start of this report clarity should be given about the notion of jurisdiction as referred to in the title and as applied in the remainder of this report. In brief: under public international law jurisdiction stands for the power of a sovereign state to regulate, to adjudicate and to enforce the norms by which its legal subjects are bound. Since this report deals with criminal issues criminal jurisdiction will be restricted to the power to regulate and to enforce, since it cannot be expected that a State would be willing to accept and to apply foreign standards of criminal law within its own territory. Criminal law in particular contains the behavioural standards that a (democratic) society esteems necessary to be obeyed or followed. Violation of these standards may therefore be followed by severe sanctions including imprisonment. Other than in the field of private law, national courts will not apply foreign criminal law in the absence of domestic regulation or if a choice for foreign law would appear more appropriate. The *Fremdrechtprinzip,* (in particular advocated in 1950-1960) was not accepted in international practise, although national courts sometimes have to consider the law of other States in matters of extradition and mutual assistance. Importation

of foreign criminal standards is only possible on the basis of international treaties followed by implementation of the related standards into domestic law.
Under public international law the principle rule it State enjoys sovereignty over its own territory. Other States should refrain from any interference with the authorities and legal order of the other State like the State involved reciprocally should refrain from interference with territorial sovereignty of other States. Under circumstances States may have legitimate reasons to assess extraterritorial jurisdiction. Paragraphs 15 ff. will be dedicated to the power of a State to regulate on its own territory, including the scope of domestic law on the basis of the known jurisdiction principles.
From there it will be analysed to what extent internet or cybercrime influence the application of these principles. One needs not to be clairvoyant to predict that a facility of internet that connects over 1.5 billion internet users on this globe[1] engaged in intense communications may not easily fit into the traditional legal approach on the assertion of jurisdiction as applied in the real and compartmented world of more or less static sovereign States.

5. A second important aspect of jurisdiction is the authority of the State to enforce its domestic law. Where, under circumstances, international public law allows to attribute with some extraterritorial effect to domestic law – as will be discussed hereafter -enforcement of domestic law on the territory of another State would amount to interference with the internal order of other sovereign States and is therefore not permitted, unless consented to by the State concerned. Consent can also be obtained by means of international agreements or treaties and can take several forms, like e.g. in Europe may happen in the form of joint police teams that operate cross-border. The internet environment seems different in the sense that it is sometimes possible to gather on-line electronic evidence that is physically located in a computer system in another territory but that is logically available – retrievable by means of software – to law enforcement authorities of another State. In principle, public international law does not permit extraterritorial jurisdiction in order to gather such (evidentiary) material. Limitations are stricter here than concerning the assertion of extraterritorial jurisdiction to regulate. The State concerned should be requested to render mutual assistance in order to provide for the material needed. Despite dedicated regulation – like in the Cybercrime Convention – intended to increase the speed of procedures of mutual assistance, this may nevertheless not always ensure the availability of the evidentiary material. This problem is further discussed under paragraphs 71 ff.

6. This report will deal briefly with principles of jurisdiction to regulate as presently known and recognised in international practice. The hypothesis is that internet – other than the real world – and the application of the present jurisdiction principles may easily lead to concurring claims of jurisdiction and thereby to conflicts of jurisdiction. That fear is not new. As will be discussed in the next paragraph the more States assert extraterritorial jurisdiction – by themselves or under the obligation of an international instrument - such an effect can be expected. The organisation of internet and internet communications makes it difficult to relate legally relevant activity to one particular territory which strengthens this effect. This report, however, is not intended to deal with jurisdictional issues in general. A first limitation is only criminal law and criminal procedural law will be considered in view of jurisdiction by a particular State or States. The second limitation is that the analysis will only take into account specificities of internet crime or cybercrime, although possible solutions may go beyond these limitations.

7. In the course of time quite a number of legal publications have addressed issues of criminal jurisdiction. In 1990 the CDPC undertook a study on extraterritorial jurisdiction and jurisdiction conflicts, providing an overview of generally accepted and recognised criminal

[1] http://www.internetworldstats.com/stats.htm . Over the years 2000 to 2008 the number of users grew by more than 300%.

jurisdiction principles under public international law and possible conflicts of jurisdiction.[2] The underlying report is extensive, accurate and detailed and refers to the standard literature on the matter in the time of its publication. I feel no need to redo this important work and therefore propose to use the content of the Recommendation as reference point for this study. One observation should be made: since the publication of the report national and international legislators reacted strongly to several attacks by international terrorism. As a consequence, the emphasis has been laid on extraterritorial jurisdiction concerning terrorist activity as an obligation in international agreements.[3] A similar reference should be made the definition of international crimes.[4] As will be argued later, this has little meaning for a type of crime like cybercrime, but it should be acknowledged that it is not impossible that a cybercrime also qualifies as a terrorist crime and therefore may be subject to jurisdiction rules as included in international instruments.

8. If more than one State asserts jurisdiction over a particular criminal act, a dispute or even a conflict may occur between the States involved. This dispute may relate to the assertion of jurisdiction as such but can also be found in factual acts by a State that prevent the other State to execute its right of jurisdiction, e.g. by not providing mutual assistance including extradition in favour of domestic proceedings.
States in dispute may decide to submit the case to the judgment of the International Court in The Hague. This is not a realistic resolution in any case, in particular where no fundamental values are at stake. In minor or cases a pragmatic solution should have the preference.

9. In literature jurisdiction conflicts may be qualified as positive and negative. A negative conflict is understood as a situation where no State is able or willing to assert jurisdiction. As follows from the next paragraphs International solidarity may require that States do assert extraterritorial jurisdiction over certain (serious) crimes. International Treaties may oblige Parties to assert jurisdiction for such cases in order to prevent that such crimes remain unpunished. Negative conflicts will only rarely occur given the increasing number of international agreements and will therefore not be further discussed.

10. If cyber crime – as will be discussed – causes an increase of concurring or competing jurisdiction claims, the question is how to resolve or better prevent these conflicts? Provided that a procedure before the International Court in The Hague for pragmatic reasons is not indicated, what alternative procedures can be proposed and what criteria can be used to weigh the jurisdiction claims of the States concerned in the relevant case? This is not a new question. The complexity of international trade and traffic already caused a closer interrelation between the legal orders of States. Criminal activity in many cases did not restrict itself to the territory of a particular State. International forms of criminality like smuggling of drugs and weapons already urged to more international co-operation and concert, including determination of the appropriate jurisdictions. It is, however, trivial that application of the traditional jurisdiction principles in the internet environment inevitable must lead – as will be sorted out *infra* - to a multiplication of possible competing asserting of jurisdiction in particular where the perpetrators of cyber crime make an extended use of internet facilities and connected computer systems, causing thereby that elements of the crime or of the criminal scheme will affect not one but a range of States. At least a number of these States may – on the basis of their domestic criminal legislation - assert jurisdiction. Whether they actually do so is another question. States may have pragmatic considerations

[2] European Committee on Crime Problems, Strasbourg 1990, 43 pages. The Recommendation contains an extensive list of standard literature on the issue. In this report only literature on specific details will be taken into account.
[3] UN Treaty of New York of December 15, 1998, UN Treaty of December 9, 1999, see also
[4] UN Rome Statute of the International Criminal Court relating to the adoption of the Rome Statute of the International Criminal Court, and the establishment of the Court, July 17, 2002.

not to investigate and prosecute a case, in particular where the crime and/or the suspect are only incidentally related to the State or where the seriousness of the crime would not justify the cost of the operation.

From a theoretical point of view the question is relevant if it would be possible to prioritise those jurisdiction claims - and in relation to that - if international regulation would be feasible and desirable.

10. A different issue is what the effect of cybercrime and internet is on jurisdiction to enforce in the light of its possible extraterritorial effects. Are the present limitations of public international law still realistic in the internet environment, what are the needs of international co-operation and would it be feasible to propose an international regulation?

11. Jurisdiction conflicts are concern for interstate relations. Concurring jurisdictions may also affect the person who would be subject of prosecutions in more than one State. This could easily lead to a cumulation of sanctions for the same crime or to prosecutions *in absenso* the result of which the defendant is not aware, but of which he will be aware if he finds himself object of a request for extradition or an arrest when visiting the State concerned. The principle of *non/ne bis in idem* as such has been incorporated in several international fundamental instruments but in those instruments it only has meaning in the national context. Instruments for international co-operation, however, may contain *non/ne bis in idem* safeguards. It should be discussed if and to what extent *ne/non bis in idem* safeguards can be directly related to prioritising concurring jurisdiction claims.

11. Understanding of new concepts and the development of theories to deal with these concepts may help to find effective and appropriate solutions, provided that the underlying problem is well-established and defined and no other solutions are at hand. The latter suggests a direction of pragmatism rather than the development of new or amended theories. Therefore, some effort should be made to make clear what jurisdiction problems may occur in cyberspace in the first place. There is one important condition or limitation: in this report those problems will only be taken into account in as far as they are typically related to internet or cybercrime – and not already common to traditional cross-border criminality – or where the intensity or frequency of the problem is particularly related to internet or cybercrime.

12. Having said so, it is desirable to discuss the concept of cybercrime that is maintained in this report and to consider its nature in relation to jurisdiction issues. Cybercrime is not a type of crime in the traditional criminal or criminological meaning. Cybercrime provisions may protect different legal interests and thereby qualify as different types of crime in the traditional sense which may have consequences for the issue of jurisdiction. Because of the organisation of the internet the commission of a cybercrime in nearly all cases is not restricted the national territory of one State. Cyber crime, apart from exceptions, is in principle a cross border crime.

13. This report is not meant as a profound scientific contribution to the theory of public international law. The ambit of the analysis is to indicate if there is a problem, and if so, in what direction solutions can be found, in particular in relation with the instruments of the Council of Europe.

14. After this introduction, the report is structured as follows:

1. Introduction (this chapter) *para* 1-13.
2. Jurisdiction to regulate, Principles (a brief description of the presently recognized principles) *para* 14-29.
3. Concept of Cybercrime *para* 30-38.
4. Jurisdiction rules in the Cybercrime Convention *para* 39-54.
5. Discussing solutions *para* 55-73.
6. Jurisdiction to enforce in the Cybercrime Convention *para* 74-90.

2 Jurisdiction to regulate, principles

15. This is now the place to provide a brief description of known and recognised jurisdiction principles as applied in the field of criminal law. In principle the same terminology is applied as used in the Council of Europe Recommendation. It should be stressed that international law does not contain general prescriptions of the reach and scope of national criminal laws. International Treaties may provide for specific rules in relation with the substantive matter of such instruments, like e.g. is also the case with the Cyber Crime Convention and its article 22. The main and most common principle is the territoriality principle which in its most simple form means that a sovereign State has the authority to judge criminal acts that have been committed in its territory. Where it comes to extraterritorial jurisdiction the CoE Recommendation[5] discerns two categories of jurisdiction principles, relating to the underlying *ratios*.[6]

Public international law and the justification of principles

Protection of State's interests	*International Solidarity*
Territoriality Principle (in addition: Flag Principle)	Unrestricted Personality Principle (including dual criminality).
Protection Principle	Universality Principle
Restricted (Passive) Personality Principle	Vicarious Jurisdiction

No strict line can be drawn between the two ratios under international law. Some principle may serve both purposes. This table can be expanded with principles that are a refinement of the categories mentioned above.

16. Territoriality principle

The main principle, of course, is the territoriality principle. This is not the place to extensively discuss what may or may not be considered as the territory of a State. It is referred to the common opinions and theories of international law (see also the discussion on article 22 Cybercrime Convention). In order to apply the territoriality principle it is necessary that the place where the crime is committed is established (e.g. by the national court in order to assert jurisdiction). It should be noted that the *locus delicti* may not be restricted to the place where the suspect acted or omitted but may be widely stretched under:

- *Ubiquity doctrine: the offence may be considered to be committed within the territory of a State if one of the physical acts constituting an element of the offence was committed there, or if the effects of the offence became manifest there (including co-authorship, aiding and abetting). Attempt, preparatory acts and conspiracy is both the place where the perpetrator intended his acts to be completed or imagined they would be completed.*

[5]

[6] General Reference: R. van Elst and A.M.M.Orie, *Jurisdiction*, in: prof.mr. E. van Sliedregt, mr. A.M.M. Orie, dr.mr. J. Sjöcrona *(eds)*, *Handbook Internationaal Strafrecht,* Deventer 2008, p. 29-91.

- *Effects doctrine (part of ubiquity doctrine): where do the acts of the offender produce effect?*

In fact, in many cases there is an extraterritorial effect under the guise of the territoriality principle. Many States apply what can be considered as the ubiquity rule: as *locus delicti* is considered every place where a constituent element of the definition of the offence has been fulfilled. The ubiquity rule may only be related to specific offences or categories of offences. This rule is sometimes incorporated in Statutes or Criminal Codes or left to national case law, and therefore subject of judicial interpretation. In fact, the notion *ubiquity* rule does not fully cover the scope of the principle. Not every effect or impact of the crime inevitably leads to court findings that the territory of any State can be considered as the *locus delicti.* The limitation is that those effects in any case must fulfil the definition of the offence.[7] A wider application may be found under the Protection Principle (see hereafter).

17. The ubiquity principle is a matter of national law and appreciation by national courts. Where applied it is embodied in national law or left to case law.[8] Seen from an international perspective application of the territoriality principle and the ubiquity doctrine provide a rather amorphous quilt pattern of potential jurisdiction claims, the key of which only can be found in national law and interpretation of the law by national courts. Since the definition of criminal offences may differ considerably between States it is hard to predict in which case a State may, or in the opposite case cannot, assert jurisdiction.

18. The CoE Recommendation in the pre-internet stage already recognizes that where communication facilities are used to commit an offences it will be difficult to determine the place of the offence. In other words, where the *locus delicti* is not evident or subject to plural interpretation there is a substantial risk that more than one State may assert jurisdiction. In order to protect the suspect, the *predictability requirement* of international public law should apply, i.e. the suspect must have been in the occasion to notice that his conduct was a violation of the criminal law of the State. Otherwise, this could be considered as an abuse of rights to claim territorial jurisdiction. Therefore, some restraint is esteemed necessary in broad application of the territoriality principle. The predictability requirement may also play a role in jurisdiction over content of websites (see para 55).

20. In relation with the previous paragraph I only mention without further discussion the principle of connex jurisdiction (Annexkompetenz) as applied in some countries.[9] National courts may assume jurisdiction over criminal acts that are closely connected to conduct over which the national court has jurisdiction. Under circumstances this may help to provide a jurisdiction basis where the *locus delicti doctrine* may not.

21. In this respect, further international harmonization of criminal offences is desirable. Since treaties or other instruments, in order to be accepted, leave Parties a certain room for implementation. Further, those instruments have often the nature of minimum requirements and are Parties to go beyond the level of obligations that they have undertaken by signing and ratifying such instruments. In my opinion, it would be useful to reconsider after a certain period of time the level of the realized harmonization and possibly take further action.

23. The *flag principle*
In fact concerns this principle extension of the national territory and application of the territoriality principle (see under paragraph 42).

---

[7] G. Gribbohm, in: Leipziger Kommentar, Berlin,, W de Gruyter, 11th edition, 1997, para 9, Nr. 19.
[8] This study does only exceptionally refer to national law and case law. At least a number of Council of Europe Member States have incorporated the ubiquity rule in national law where in other states courts rely on case law.
[9] See e.g. Germany, Belgium.

24. *Protection principle*
The protection principle may be invoked to defend serious national interests. Sometimes the notion of *essential interests* is used. How to interpret serious or essential is open for national appreciation. No common standards have been developed. By its nature, the protection principle will only be applied to specific (serious) crimes. There need not to be a connection (nationality) with the prosecuting State; it will be applied in those cases where the territoriality principle will not provide a basis for jurisdiction (acts fully committed outside the national territory) and no double criminality requirement.

24. Passive personality principle
A State may wish to protect the private interests of its citizens or residents by enacting relevant criminal offences. Again, the nature of this offence must be serious enough to justify the extraterritorial effect of the principle. The perpetrator of such an offence is any person – irrespective his or her nationality – who illegally interferes with these interests. And where the principle that applies is for example the criminalization of sexual contact with minors, irrespective of the place where the act takes place. In order to protect the rights of the suspect in most cases dual criminality is required, i.e. the act must be criminalized both under the law of the territory State as well as under the law of the former State. Application of this principle may easily bring concurring jurisdiction claims. In literature no consent can be found about a possible additional requirement that jurisdiction should be left tot the State with the most favourable law to the defendant (in particular concerning possible sanctions).

25. A*ctive nationality principle*
A State may extend the scope of its national criminal law to conduct committed by its nationals. It may be discerned between the absolute active personality of nationality principle, the unrestricted active personality principle and the restrictive active nationality principle. The first principle means that a State makes its national law applicable on its nationals wherever they find themselves. The restrictive variant means that some criminal acts are made applicable to nationals irrespective as to whether the conduct is criminalized under the law of *locus fori.* The last variant does require dual criminality. All variants can be found in national laws, relating to a specific crime, category of categories of crime. In general sense it can be said that the last variant seems to be the most common concept in national laws. It should be pointed at difficulties to establish dual criminality because there is no consensus about the criteria to consider (e.g. time of enactment of the law, fulfilment of general conditions to assume criminal liability of definition of offences containing elements that cannot be fulfilled outside the national territory). Here is not to explore criteria applied in national law to establish dual criminality nor the place to discuss the justification of these principles. It suffices to assume that application of one or more of the variants of the principle easily may lead to concurring claims of jurisdiction.

26. *Principle of derived jurisdiction (vicarious jurisdiction)*
This is not an independent basis for jurisdiction. A State that has no jurisdiction over certain acts according to its national law or case law and embodied principles, may assume jurisdiction if the State that has (originaire) jurisdiction so determines. This can be done in the form of a formal request or on the basis of an international treaty.[10]

27. *Universality principle* (Weltrechtsprinzip)
This principle is the most far-reaching jurisdiction principle that combines the scope of the territoriality principle, the active and passive personality principles, without specific restrictions as under the protection principle. The risk that application of the principle will be

[10] See e.g. article 2 ss 1, European Convention on the Transfer of Proceedings in Criminal Matters, May 15, 1972, CETS 73.

experiences as interference with internal affairs of another State is not unlikely. Application of the principle therefore requires specific justification and restrictive application, like in case of international crimes.

28. The Conclusions of the CoE Recommendation of 1990 were:

- Public international law does not pose restrictions on State's freedom to establish forms of extraterritorial criminal jurisdiction concerning the fighting of crime.
- On most principles there is no common international understanding, not amongst the national courts when applying national law, not in international literature.
- Attention should be paid to the prevention of jurisdiction conflicts because that would undermine international solidarity. Most of such conflicts are due to application of the protection principle (including variants), or due to extensive interpretation of the territoriality principle (read: ubiquity doctrine).
- Conflicts of jurisdiction arising from application of the principle of passive personality (nationality) – nationals or residents are victim of the crime imply a distrust of level and quality of law *locus fori* and suffer from insufficient forseeability for the suspect of the crime.

Further, international public law does not provide standards to what extend States have the right to determine the scope of their national criminal law *ratione loci*, but is it true that public international law sets limits on the extent to which states may assert extraterritorial jurisdiction, as reflected in quite a number of mainly American, English and German scientific publications. Nevertheless, those standards and norms are rather vague. Basic concepts of sovereignty and equality imply that limitations of extraterritorial jurisdiction have to be accepted in order to prevent unacceptable intervention in the internal affairs of other states.

29. The CoE Recommendation proposes a number of actions and mechanisms that will mentioned hereafter briefly.

- Unilateral action by the States concerned, i.e. restrictive application of principles that lead to extraterritorial jurisdiction claims; internationally[11] a *ne bis in idem* should be recognised and a criterion of reasonableness should be applied when considering to exercise jurisdiction.[12]
- Unilateral enactment of defensive laws against unwanted extraterritorial claims of jurisdiction by other States. This can amongst other things be realised in specific restrictive provisions in (bilateral) agreements on mutual assistance including extradition.
  - Such blocking measures seem not to serve the concept of international solidarity.
- Multilateral Mechanisms like[13]
  - Harmonisation of national substantive criminal laws.
  - Consultations concerning new law projects.
  - In principle it is not a bad idea to consult parties before enacting laws, but I am afraid that this idea is too idealistic and not very pragmatic.
  - International agreement on a transnational rule of *ne bis in idem*.
    Indeed this is still the most important suggestion. The Recommendation refers to Council of Europe Instruments that contain a reference to the *ne bis in idem* rule, but in a negative sense, i.e. as ground for refusal of international co-operation. As a

[11] To avoid misunderstandings, what is actually meant is a *transnational* effect the ne bis in idem rule (see hereafter paragraph 68).
[12] European Committee on Crime Problems, *Extraterritorial criminal jurisdiction,* Strasbourg 1990, p. 30-31
[13] Ibidem, p. 32-36.

positive criterion it is embodied in two other CoE Conventions that met little enthusiasm among the Member States.[14]
A complicating factor is what exactly should be considered as "the same act" in the sense of those provisions. In relation thereto see paragraph about interpretation of a similar *ne/non bis in idem rule* in the Schengen-arrangement of the European Union.

- International agreements concerning the transfer of proceedings.
  Despite the low number of ratifications, this Convention could be an important instrument in preventing (and resolving) concurring jurisdiction and possible conflicts.
- Arrangements for the settlement of jurisdiction conflicts.
  The Recommendation recognises that States are not willing to submit conflicts to the International Court of Justice, in particular if no practical circumstances prevent a parallel prosecution. Nevertheless, States should show the preparedness, also on behalf of the suspect, to look for bodies or ways to deal with a possible conflict. Of course, the European Committee on Crime Problems is proposed to take the role of advisory body on the matter.
  The report does not provide concrete criteria how to resolve possible conflicts of jurisdiction apart from general remarks on the primacy of the territoriality principle, the equality between participants in international intercourse and the need for mutual respect for the integrity of these participants, the principle of non-intervention and the requirement of predictability in relation to the *nulla poena* rule.

3 The concept of cybercrime

30. Cybercrime is a broad notion. In literature all kind of definitions can be found of computer crime, computer-related crime, internet crime, etc., including discussions what about which specific crimes should be considered as such. In my opinion, the notion of cybercrime should be considered as a so-called container notion: what is in the box depends very much from the needs and considerations of the person who is filling it and may even be subject to change over time. Since the emergence of internet after 1995 as mass means of communication it appeared possible to set up all kind of fraud and deceit by making use of the internet. The scope of what should be considered as cybercrime is thereby considerably enlarged. Therefore, modern definitions of cyber crime describe cybercrime as concerning any crime for the commission of which the use of the internet was essential. The implies that even offences that do not include an explicit reference to ICT or to the electronic environment, can nevertheless be considered as such if the criminal conduct was directed against other computers or where the facilities of the internet were used to disseminate or retrieve information. 'Essential' means that ICT or the electronic environment is an essential element of the criminal conduct. A murder in the computer room would not qualify as such.

31. Under the notion of cybercrime all kind of subcategories can be distinguished, including their refinements and details. In order to be able to make observations about the impact on criminal jurisdiction, it is necessary to define some broad subcategories. The Cybercrime Convention 2001, that adopted the notion of cybercrime, does not provide a definition but distinguished in its substantive law part four categories of cybercrime:

a) c.i.a-offences: dealing with conduct that is directed against computer systems (and networks) and the data processed, stored or transferred by it;
b) computer-related offences, property crimes committed by means of computer systems

[14] European Convention on the Transfer of Proceedings in Criminal Matters, 1972, articles 35 to 37, CETS 073, at present (March 2009) 25 ratifications and 10 signatures.
European Convention on the International Validity of Criminal Judgments, articles 53 to 55, CETS 070, at present (March 2009) 10 ratifications and 7 signatures.

c) content-related offences, concerning the disclosure or making available by means of a computer system of illegal content; and as a separate category
d) offences related to intellectual property.

For the purposes of this report it is not necessary to maintain a separate category d), which here can be largely taken together with category c).

32. Category a) will generally spoken deal with illegal conduct that may cause damage or other unlawful effects in computer systems or in relation to data contained therein. There is at least a potential nexus with the territory where the perpetrator acts, but also one with the territory where the damage occurs and is felt by the owner or user of the computer system. In case of viruses or other malware the attack may not be specifically directed at an individual system or data collection, but may be felt by a large group of victims. It should therefore be discussed if under which circumstances a nexus can be established with the territory of a state.

33. Category b) represents so-called assimilation clauses, i.e. parties to the Cybercrime have to see that their system of property crimes also applies in the electronic environment. Parties may enact legislation that is more detailed or more specific, e.g. concerning identity theft. In general terms, criminal conduct in this category is mostly directed against a specific victim unless e.g. the domestic legislator would have enacted pre-stage offences that are aimed to prohibit preparatory actions.

34. It should be pointed at that category c) in fact is an open category. At present the Cyber Crime Convention and its 1st Additional Protocol only cover a limited number of content-related crimes, at present restricted to child porn and racism and xenophobia. One could imagine that other criminal activity would qualify as content-related crime as well.[15] An important element of category c) often will be the making available or offering of illegal content by means of a website or usenet-forum. In principle, the content of an open website is available to any internet-user. This would mean that the effect of illegal content can be felt anywhere, it means in any State. If this would lead to assertion of jurisdiction by the States concerned on the basis of the one or more of the discussed jurisdiction principles as incorporated in national law or adopted in national case law it could lead to jurisdiction conflicts.

35. Together with the opportunities to obtain illicit profits on the internet it seems that there is a tendency or shift from individuals committing computer-vandalism or causing nuisance to more organised group activity. For the purposes of this study, it is not particular interesting if those groups meet the conditions to be qualified as criminal organisations or not.[16] The trend to be pointed at is that the criminal intent of the perpetrators, in particular those organised in groups, is no longer to commit an individual or specific cyber crime but to set up a criminal scheme, for the realisation of which several cybercrimes and other crimes are committed.

[15] See e.g. *grooming, offering pharmaceuticalproducts without prescription, illegal gambling, but also the offering of stolen or other illegal goods.*
[16] R.C. van der Hulst/R.J.M. Neve, High-tech crime, soorten criminaliteit en hun daders (High-tech crime, categories of crime and their perpetrators), The Hague 2008 p. 152 (summary in English).

36. An example of a cyber crime with international implications:

On the internet botnet software is bought with the parameters set for the use intended. The bot is send around by means of infected e-mail. E-mail -addresses are generated. If the addressee opens the mail a virus or trojan installs the bot in the computer system of the unaware user.
The bot collects its instructions from a website installed by the criminal group.
The botnet can be used to send out spam (for financial compensation), to send out phishing mail containing falsified data and when a user provides it financial data the actual fraud scheme can be carried out.
The bot can be used to spy in the computer system (pass words and financial data).
The botnet may also be used to launch DDoS-attacks to other computer systems connected to the internet.

As part of this criminal scheme a number of cybercrimes are committed, like illegal access, possibly followed by illegal use, data manipulation by installing a bot, interference with data flows, computer sabotage, computer forgery and computer fraud, etc., but also traditional crimes like theft, embezzlement etc. may be part of the criminal scheme.

Another example:

A perpetrator tries to hack (a) into a specific computer system. He (or she) may do so in order to spy and/or copy data, in order to use the processing capacity of the system or to halt the system (b). He may even do this with the intent to blackmail the system owner and agree a ransom for not sabotaging the system or to obtain illicit financial profits (c). Elements of this criminal scheme indicated as a) and b) and possibly c) are only covered by the substantive provisions of the Cybercrime Convention, the other conduct probably will be covered by classical criminal provisions or by specific domestic cyber crime offences.

Even clearer:

In a case of phishing false e-mails are send out to collect access codes and pass words that would enable the perpetrator to transfer money form that account, or brings the sender of the mail in contact with the victim in order to make him transfer money. The first part of the scheme is internet related, the second part is probably criminalised under traditional criminal provisions.

37. The findings from the previous paragraphs are:

- the criminalisations under the Cybercrime Convention , in particular category b) and c) are not exhaustive. National law may criminalise conduct that has not been defined or addressed under the Cybercrime Convention.
- today, criminal schemes involve a number of different crimes that may qualify as cybercrime and as well as traditional crime.
- the effect of the commission of a crime in any category may be experienced by any internet user en therefore in any State. In theory, any State could assert jurisdiction over the crime, depending from the adopted jurisdiction principles under its legal system as elaborated in relation to certain offences.
- (legal) measures in order to limit the number of concurring jurisdiction should take into account that cyber crime and traditional crime cannot and should not be treated differently, al least not where it comes to jurisdiction.

4 The jurisdiction provisions in the Cybercrime Convention 2001

38. Article 22 obliges Parties to establish jurisdiction over the offences defined by the Convention in its article 2-11 (EM 232). This includes the technical offences (c.i.a-offences) as well as the computer-related offences, the content-related offences and the intellectual property offences. Article 11 refers to aiding and abetting of these crimes and is therefore included. Article 12 provides for (criminal liability) of legal persons and is not referred to in article 22. Where Parties do attach criminal liability both to legal and natural persons it seems logical to extent the jurisdiction principles of article 22 to offences as defined in articles 2-11 committed by legal persons as well. Since Parties may choose to implement civil and administrative liability instead of criminal liability, the inclusion of article 12 in the scope of article 22 would not necessarily enable the kind of international co-operation desired. Moreover, aiding and abetting to the offences of article 2-10, as provided for in article 11, is included.

39. Article 8 section 1 of the First Additional Protocol to the Convention (2003, CETS 189) makes art. 22 of the Convention – of course to the extent implemented by the individual Parties - fully applicable to the offences of the Protocol as well. Therefore there is no need to spend specific attention to jurisdiction principles in relation to the offences defined by the Protocol. If the nature of the cyber crime would be relevant for which jurisdiction principle to apply, the offences of the Protocol best could be treated in a similar way as article 9 (content-related offences) under the Convention.

40. Although it was largely recognised in literature that *cyber space* is very much different from the real world of flesh and blood and that one of the main characteristics of *cyber space* is its borderless nature. The question whether or not this would bring a need for the development or adaptation of jurisdiction principles to be applied in this *cyber space* only was answered negatively by the drafting committee of the Cybercrime Convention for obvious reasons. Criminal law deals with conduct of natural persons. That conduct may be realised by means of computer programs or by means of computer communications. Notwithstanding the nature of these crimes, the responsible perpetrator is a person of flesh and blood who at a determined moment of time and at some specific physical location initiates his criminal scheme. It is true that this initial step may consist of the launching of a simple key stroke command, and that the impact of his action may be felt much hours or day later at numerous other physical locations. This, however, does not do away with the physical presence at a certain moment of time of the perpetrator in the territory of a State, nor does it mean that the consequences of perpetrators act will not be felt by other persons, at that moment present in the territory of the same or other State. Secondly, it was not manifest that traditional theories and principles of jurisdiction would not be applicable in such cases of cybercrime. In addition, it was assumed that most cybercrime acts would not only consist of mere virtual activity but would be a combination physical activity and other activity within the virtual cyber space. And at last, where legal theory in international public law developed jurisdiction principles that already demonstrated adequate flexibility in a world where international transactions and global communication systems already obtained an important place. At the time, there no need was felt for the development of alternative jurisdiction principles in a world where these principles would have to be applied in combination of or in place of the traditional ones that proved their values.

41. The main jurisdiction principle chosen in the Cybercrime Convention therefore is the territoriality principle. Despite the special nature of cybercrimes an important number of cyber crimes will be committed by a perpetrator against a victim where both reside within the territory of one State. Or, where the attacked computer system is located within a

particular State, irrespective the location where the perpetrator acts. As will be discussed later, the territoriality principle enables to assert territorial jurisdiction over such criminal conduct.

42. As commonly accepted in public international law, a variant of the principle of territoriality includes ships and aircrafts registered under the law of that Party (flag principle, see article 22 paragraph 1(b) – (c). These variant is usually applied in domestic law. The Cybercrime Convention obliges its Parties to extend the scope of this principle to cybercrimes as well. If the cyber crime is committed on a ship or aircraft that is beyond the territory of the flag Party, there may be no other State that would be able to exercise jurisdiction if this requirement would not be in place. Further, if a crime is committed aboard a ship or aircraft which is merely passing through the waters or airspace of another State, the latter State may face significant practical impediments to exercise its jurisdiction, and it is therefore useful for the State of registry to also have jurisdiction.

43. Concerning article 22 the question was studied if a cyber crime could be committed outside the territorial jurisdiction of any State, and if so, if article 22 should oblige Parties to the Convention to assert jurisdiction over such cases in order to avoid loopholes in the system of international enforcement of cyber crime. Two cases were studied: a) If a cyber crime would involve a satellite, and b) if a cybercrime would e.g. involve a non-registered ship at the High Sea. It is clear that these cases rather have theoretical value than significance in daily practice, but answering questions like these contributes to the finding of balanced solutions. Concerning a) it was studied if registration – like with ships and aircrafts - was an appropriate basis for asserting criminal jurisdiction. Since a satellite serves as a mere conduit for a transmission, in many cases there would be no meaningful nexus between the offence committed and the State of registry. In addition, it is most likely that as well as the sender of the satellite communication and the receiver of that communication will find themselves somewhere in at a physical location in a territory, where a State is able to assert jurisdiction over the criminal act. Concerning case b) it was recognised that under certain circumstances no State would be entitled to assert jurisdiction. Nevertheless, this case was considered as mere theoretical. Moreover, paragraph 4 of article 22 does not exclude the application of other jurisdiction principles by an individual Party over such situations. In addition, it can be referred to paragraph 1, littera d (see hereafter), that encompasses the nationality principle and could be applied in the case referred to.

44. Paragraph 1, *littera d* reflects the nationality principle. The nationality theory is most frequently applied by States applying the civil law tradition. It provides that nationals of a State are obliged to comply with the domestic law even when they are outside its territory. Under *littera d*, if a national commits an offence abroad, the Party is obliged to have the ability to prosecute it if the conduct is also an offence under the law of the State in which it was committed even if the conduct has taken place outside the territorial jurisdiction of any State. In relation with cyber crime application of the nationality principle is important in two manners. It prevents nationals of a State to travel to a foreign State to commit a cyber crime and afterwards return home without the risk of being prosecuted. The principle also asserts jurisdiction over locations where no State asserts jurisdiction, like discussed in the previous paragraph.

45. Article 22, paragraph 2 allows Parties to enter a reservation to the jurisdiction grounds laid down in paragraph 1, *litterae b, c*, and *d*. It is clear that this reservation possibility, necessary because of lacking consensus on the scope of national jurisdiction, may weaken the proposed jurisdiction system of article 22 if Parties to the Convention would decide to go for a minimal implementation.

46. Actually, given the present number of ratifications of 23 Parties at Nov 10, 2008 , only three Parties did make use of the reservation possibility on article 22: France does not assert jurisdiction over locations where no State has jurisdiction, which is only a partly reservation on article 1 *litera* d. Further France raises the condition that proceedings in France will only be undertaken upon request of the other State, to be preceded by a complaint of or on behalf of the victim. Latvia does not apply the whole of paragraph 1 under d. U.S.A. declares that it cannot provide for plenary jurisdiction i.e. systematically. Whether or not jurisdiction can be asserted over offences committed in cases b, c or d is dependent from regulation its federal law. In most cases , where a federal interest is at stake, the federation has jurisdiction in case of article 22, paragraph 1 literae b, c and d.

47. The preliminary conclusion is that the majority of Parties will apply the proposed jurisdiction system of article 22 paragraph 1-2 to the full extent. The reservations made only concern a small fraction of cases.

48. Paragraph 3 of Article 22 recalls the internationally accepted principle *"aut dedere aut judicare"* (extradite or prosecute) i.e. in cases where that Party has refused to extradite the alleged offender on the basis of his nationality and the offender is present on its territory. Jurisdiction established on the basis of paragraph 3 is necessary to ensure that those Parties that refuse to extradite a national have the legal ability to undertake investigations and proceedings domestically instead, if sought by the Party that requested extradition pursuant to the requirements of "Extradition", Article 24, paragraph 6 of this Convention. Modern extradition laws more than before allow the extradition – in serious cases and under conditions – nationals. The rule nevertheless remains meaningful.

49. Article 22 refers to the principle of territoriality as the basis of jurisdiction of a Party. Territory should be understood in a broad sense, i.e. including ships and aircrafts. Paragraph 2 introduces a restricted nationality principle and paragraph 3 obliges Parties to assert jurisdiction where extradition of nationals is not legally possible. In addition, paragraph 4 of Article 22 permits the Parties to establish, in conformity with their domestic law and legal principles, other types of criminal jurisdiction as well. In this sense Article 22 is not exclusive. However, applying of other jurisdiction principles may lead to competing jurisdiction claims and therefore to jurisdiction conflicts.

50. In the case of crimes committed by use of computer systems, there will be occasions in which more than one Party has jurisdiction over some or all of the participants in the crime. For example, many virus attacks, frauds and copyright violations committed through use of the Internet target victims located in many States. In order to avoid duplication of effort, unnecessary inconvenience for witnesses, or competition among law enforcement officials of the States concerned, or to otherwise facilitate the efficiency or fairness of the proceedings, the affected Parties are to consult in order to determine the proper venue for prosecution. In some cases, it will be most effective for the States concerned to choose a single venue for prosecution; in others, it may be best for one State to prosecute some participants, while one or more other States pursue others. Either result is permitted under this paragraph. Finally, the obligation to consult is not absolute, but is to take place "where appropriate." Thus, for example, if one of the Parties knows that consultation is not necessary (e.g., it has received confirmation that the other Party is not planning to take action), or if a Party is of the view that consultation may impair its investigation or proceeding, it may delay or decline consultation. A similar provision can be found in the UN-Convention on Transnational Crime.

51. From the discussion above and the daily practise of public international law it must be concluded that the criminal policy of States in general is not intended to expand national jurisdiction as far as possible. Extraterritorial jurisdiction in most cases will only concern

internationally recognised serious crimes – in particular where obliged by specific international treaties. Further, most commonly States adhere to the Protection Principle and the (Restricted) Nationality Principle. In the case of Cybercrime and internet, where the perpetrator need not to be in the physical presence of his victim and where he uses the facilities of internet to commit the crime – once or repeatedly – the criteria that usually are applied by domestic courts to determine the place of the commission of the crime (*locus delicti)* may easily lead to the situation where several States could assert jurisdiction over the same criminal fact of facts.

52. A preliminary conclusion to be drawn from the discussion of jurisdiction principles in combination with the nature of Cybercrime is that, on the basis of the traditional criteria, it may be very difficult to determine the most appropriate jurisdiction to prosecute a case. Actually, we could say that somewhere on the internet we could find acts or elements that together form the cybercrime in question. May be, some of these elements can be brought in connection with a physical location, e.g. if certain data is stored in a particular computer system or if a particular program in a particular computer is used for certain processing functions. Seen from the internet perspective these relations may appear to be rather incidental than instrumental. They may also be very numerous. Spreading malicious software over the internet by means of botnets may involve millions of e-mails sent out. As a matter of speaking the elements of such crimes form an intransparent cloud. At the same time, more than one State could assert jurisdiction over specific elements of the crime that it considers to have a nexus with its territory or legal order. If States indeed assumes jurisdiction is an open question. At present there no statistics are available that indicate that jurisdiction conflicts are occurring frequently and that those conflicts will occur more frequently in the near future.

53. In literature principles and criteria are proposed to restrict *ubiquitous* claims of jurisdiction. Introduction of specific internet principles like preference for the personality principle and an adapted flag principle in addition to a (unrestricted) territoriality principle have proven to be a too restrictive approach.
The same goes for a proposal to give priority the law of the State where the access-provider is located. This may cause problems, in particular where internet users chose providers in countries in States where certain conduct is not criminalised where it is in other States including the home State of the internet user and it ignores that in complex criminal schemes more providers and internet users may be involved.

54. National courts in the meantime have shown ample reserve in accepting the full consequences of *locus delicti* and the ubiquity criterion where it comes to information that is made available at a website, located on a server in a particular State. This is not the place to discuss the role and responsibility of the service provider. In theory it is possible that the making available is not criminal in the first State but it is (because its effect) in the second or the other way round, the making available can be criminalised in both States, and the effect of the information can be criminalised in both States. Ultimately, both States could be considered as the *locus delicti* of the crime. Courts may not accept this unconditionally. Several criteria are adopted like where the receiver is voluntary or involuntary confronted with the material ('push and pull" techniques), but also the criterion of 'directed at' (e.g. following from the language used) in addition to criteria on foreseeable or intended harm. The impression from case law[17] is that courts decide on a case by case basis. Protection of the own legal order or interests of nationals and residents still plays a dominant role.[18]

[17] See e.g.Utah Kohl, Jurisdiction and the Internet, Cambridge University Pree 2007, p 97 ff and p. 253 ff.
[18] See e.g. the Toben Case in Germany, December 12, 2000, 1 StR 184/00. Yahoo case, Tribunal de Grande Instance Paris, August 11, 2000.

5 Discussing solutions

55. The first question to be answered is whether there is a problem that requires immediate action? A second question is in how far such actions should or can be undertaken by the Council of Europe? To this purpose I take the action points as proposed in 2009 (see paragraph 28) as starting point.

56. The Recommendation of 1990 calls the Parties to give a restrictive application to jurisdiction principles that lead to extraterritorial jurisdiction. As demonstrated above, the main sources of extraterritorial jurisdiction are the territoriality principle (sic!), the personality principle(s) and the protection principle. Undoubtedly, cyber crime, often being a transborder type of crime, contributes to the number of extraterritorial jurisdiction claims but so does the internalisation of social and commercial intercourse as well. It has been argued in literature that the traditional jurisdiction principles lead to overly broad jurisdiction for national courts and that those principles are outdated in today's international society. Development and the introduction of new concepts – if feasible at all - goes beyond the scope of cyber crime and cannot be realised by the Council of Europe's and its member States alone.

57. If a State asserts jurisdiction over a cyber crime is dependent from a number of factors. Apart from principle considerations that a State could have to prosecute, there are many practical factors that may prevent effective prosecution, such as the formal or factual impossibility to obtain the required mutual legal assistance. Sometimes, national law obliges the prosecution service to investigate and prosecute crimes come to their knowledge where other legal systems provide the prosecution service with an discretionary authority to refrain from prosecution because of general or specific interests. Where should be aimed at restriction of extraterritorial jurisdiction, also related issues should be taken into account.

58. The expectation is in the near future many jurisdiction disputes will arise. It is my experience that, States apply adhere to pragmatism in dealing with jurisdiction issues and possible conflicts that would arise from it. It is unlikely, impractical and counterproductive if Parties to the Cybercrime Convention, instead of having a mutual consultation in order to determine the most appropriate jurisdiction, would invite the International Court of Justice in the Hague to rule on a conflict of jurisdiction.[19] Sometimes, national interests proscribe the maintaining of a claim of jurisdiction, including procedural requirements that demand the prosecution services to prosecute a crime committed within the national context. No concrete statistics are available on the number and expectation of concrete cybercrime related jurisdiction issues in the future. Further, restrictions and guarantees in other international co-operation instruments like on Extradition and on Mutual Assistance may already prevent that a prosecution can be undertaken in more than one State if co-operation is necessary for a successful criminal prosecution.
Since it obviously is expected but not known if it is realistic that many internet related jurisdiction problems will occur, it may be wise to look at mechanisms that can help to resolve possible jurisdiction disputes and conflicts. Additionally, other measures could be considered to protect the interests of the defendant who is subject of multiple jurisdiction claims. To this end the Recommendation of 1990 promotes the enactment of an

[19] The Court envisages a strong grow of the number of cases, the agenda mainly consist of traditional conflicts territorial and maritime disputes and other conflicts in the frame of international agreements. Internet cases have not (yet) been reported (http://www.icj-cij.org/presscom/index.php?p1=6&p2=1).

international agreement on *ne/non bis in idem*. This point will be taken up in a separate paragraph 68.

59. One of the suggestions of the Recommendation of 1990 was to make arrangements for the settlement of jurisdiction conflicts. Article 22 of the Cybercrime Convention provides for a mechanism of consultation. It has met criticism for not providing concrete criteria to solve possible conflicting claims of jurisdiction. Indeed, neither the legal text nor the Explanatory Memorandum of Cybercrime Convention do provide (substantial) guidance how Parties can or should prioritise concurring claims for jurisdiction over the same offence.[20] Article 22 is in this respect rather similar to article 15, para 5 of the UN Convention against Transnational Crime that neither does contain concrete indications or prescriptions how potential conflicts can be solved. The UN-provision, however, is slightly different than article 22, *para* 5 of the Cybercrime Convention. The former provision calls upon Parties to the Convention to consult each other in view to coordinating their *actions* which may concern different phases of criminal proceedings, including the investigation and the prosecution. The Cybercrime Convention, in its article 22, refers to consultation with a view to determining the most *appropriate jurisdiction*. The wordings *appropriate* refer not only to practical issues but also to inherent legitimate interests of witnesses and suspects. State Parties should consider, when choosing a venue for prosecution not only the efficiency but also the fairness of the proceedings.[21] This restriction in article 22 CCC compared to article 15 CTC is justified because the existence of the European Conventions in the field of international co-operation in criminal matters.

60. It has further been argued that the traditional criteria that would be applied to prioritise jurisdiction claims in the real world would loose their distinctive meaning in the internet environment.[22] In particular, internet connections enable cyber criminals to act or initiate actions from several locations which would make it difficult to determine one or the main *locus delicti.* In addition, as also has been indicated above, cyber crime is often part of a complicated criminal scheme that may involve more that a single offence.[23]

61. Is it possible to provide for criteria to prioritise concurring jurisdiction claims? The authors referred to in the previous paragraph advocate the elaboration of such criteria. They considered criteria that helped to solve classical cases of jurisdiction conflicts under reference to the *Princeton Principles on Universal Jurisdiction*[24] , in particular Principle nr. 8 on Competing National Jurisdictions. [25] The authors of the Principles referred to were convinced that a pre-ranking of these criteria should not be given, although it is clear that some criteria do weigh more than others. The criteria, if relevant, could be used to determine the appropriate jurisdiction on the basis of an *aggregate balance* (curs. HK) of these factors. Although the jurisdiction of universality will not be frequently applied by Parties to the Cybercrime Convention, the assertion of jurisdiction on the basis of other principles, as well as the interpretation of *locus delicti* may, in certain cybercrime cases, *de facto* come down to universal jurisdiction. On the other hand, the Princeton Principles deal with crime in general and do not take into account the specifics of Cybercrime.

---

[20] Bert-Jaap Koops, Susan W. Brenner (ed), Cybercrime and Jurisdiction, A Global Survey, Information Technology & Law Series, vol 11, Asser Press, The Hague 2006, p. 330.
[21] Explanatory Memorandum, *para* 239.
[22] In particular: Bert-Jaap Koops/Susan W. Brenner, Cybercrime and Jurisdiction, The Hague 2006, p. 329-346.
[23] Ibidem, p. 326.
[24] http://www1.umn.edu/humanrts/instree/princeton.html
[25] Principle 8 deals with a specific situation: Where more than one state has or may assert jurisdiction over a person and where the state that has custody of the person has no basis for jurisdiction other than the principle of universality.

62. An important factor/criterion remains to be (a) the place of commission of the crime. I do not agree that this criterion would loose it predominant meaning for the assertion of jurisdiction in cybercrime cases, because a cyber offence is initiated by the perpetrator usually standing in his shoes on the territory of a particular state. Of course, in theory it is possible that similar actions are undertaken at another location (internet café?) in another jurisdiction. If one location is more relevant for the commission of the crime depends from factual circumstances. Whether the act has international implications or not national legal order has been affected because the violation of national law. In this respect the criterion of the place where the initiation or the commission of the crime took place keeps it value, although it must be said that States for pragmatic reasons may waive their right t execute jurisdiction. Secondly, the effect of the cybercrime may be experienced by one or (much) more victims, who themselves or whose victimized computer systems are present at the territory of another state or states. These States may expect some preference in exercising jurisdiction over the offence. (b) Custody of the suspect. In case a cybercriminal is arrested in a particular State and given that his acts caused damage to (computers of) persons in that State but also in other States, those other States may not be satisfied with a criminal prosecution in the first State, e.g. in cases where the offender made numerous victims or caused extreme damage in the latter State. The Custody-criterion could be given more weight by taking into account the course and the efforts undertaken within the frame of the criminal investigation that lead to the arrest of the suspect.

63. Of course, the harm-criterion may be decisive with regard of the solving or preventing of jurisdiction conflicts. Harm in the meaning financial and other damage, the number of computers affected etc. In my opinion also the nature and the seriousness of crime provide a measure for harm, i.e. the infringement upon national legal order. The amount of harm concerning cybercrimes is difficult to assess, because (some or many) victims may not even report the case. Given the rather so-called high black number of cybercrime cases the harm-criterion will usually work in favour of the State that has custody of the suspect or is the place where the crime was committed. Other States may have problems in adequately demonstrating the harm that occurred in their territory. In addition, in most cybercrime cases the court is convinced that the alleged conduct of the suspect caused damage because of the application of certain malware or by sending infected message to the public rather than that it requires to proof the exact and the full amount of damage.

64. In prioritising jurisdiction, the nationality of the victim has possibly less relevance. Attacks to computer systems and data stored in it are usually not directed against persons of a certain nationality. Further, persons involved in attacked systems may have a range of different nationalities. The nationality of the suspect may be relevant, depending from the elaboration of the personality principle under national law. Since this principle is supposed to reflect international solidarity it deserves weight.

65. Other factors to be considered are the likelihood of a successful prosecution (evidence, witnesses). From a Council of Europe perspective, the quality and safeguards of local procedures should be taken into account, in particular respect of human rights and e.g. the possibility to transfer the convicted person to his home country to serve his punishments.

66. Building upon the Recommendation of 1990 a solution could be to involve the CDPC as a competent body to prioritise jurisdiction claims. Firstly, the involvement of the CDPC could help to collect information about the size and the seriousness of the problem, and the CDPC is capable to propose a ruling in view of the relevant instruments in force between the Parties. The CDPC has ample experience with international co-operation and its involvement is already formalised in article 45 of the Cybercrime Convention. However, to give the CDPC a clear role, ss 2 of article 45 would need to be broadened. Article 22 ss 5 refers only to the

offences defined under the Convention. An additional sentence in ss 5 should refer to the mechanism of article 45. Parties may agree that the CDPC provides a binding ruling but they may also agree to receive an advice for further consideration. It should be discussed if intervention of the CDPC is mandatory and if Parties should agree to a binding ruling. The convention could contain an obligation to report cases. In principle, I see no objections that third parties agree to submit jurisdiction conflicts with Council of Europe members to the CDPC.
From there, the mechanism could find its place in future Council of Europe instruments Already article 29 of the Preliminary Draft Convention on Counterfeiting on Medical Products[26] is a step in that direction.,

67. The Recommendation of 2009 suggests that more use should be made of the 1972 Convention on the Transfer of Proceedings. Concerning Cybercrime law enforcement of different States and Parties often co-operate and share information concerning the investigation of criminal schemes that have international proliferation. E.g. the investigation of child porn cases or serious fraud cases. If the evidence has been obtained and the suspects are known or apprehended, it seems possible to take a decision about the forum of prosecution of the suspects. If, as a result of that, the proceedings are formally transferred to the most appropriate Party, the transferring Party waives its right for prosecution and the defendant could be given under a ne bis in idem rule. Because of the rights of the defendant this should be a formal transfer and not a pragmatic informal agreement between law enforcement authorities. Not in all cases it is necessary that the transfer vests jurisdiction of the receiving Party. In this respect it is recommended to study the possibility for a comprehensive set of rules that would enable to transfer proceeding and grant ne bis in idem, e.g. as part of the Cybercrime Convention for a start, in particular because the Parties of this Convention may not be Members of the Council of Europe.

68. *Ne/non bis in idem*
In several international instruments the right of a defendant is laid down not to be object of a criminal proceeding concerning facts concerning which he has been prosecuted and convicted in a preceding criminal procedure. This right is formulated in subsection 7 of article 14 of the International Covenant on Civil and Political Rights (New York, December 19, 1966) Ne bis in idem is also incorporated in article 4 of the 7th Protocol (Strasbourg, November 22, 1984) to the European Convention for the Protection of Human Rights and Fundamental Freedoms (Rome, November 4, 1950). The 7th Protocol is ratified by 41 CoE Member States, signed but not ratified by another 5 and not signed by 1 Member State.[27] Both articles relate to *ne bis in idem* concerning criminal prosecutions within a Contracting Party to the Convention. In theory this would leave room to start another, second criminal procedure in another State concerning the same facts and therefore it is necessary to include incorporate the *ne bis in idem* principle in other European Conventions as well, like in article 9 of the European Extradition Convention (December 13, 1957, as amended by article 2 of its Protocol of October 15, 1975[28]), in article 53 or in article 6 *littera* d) *iuncto* article 53 of the European Convention on the International Validity of Criminal Judgements (May 28, 1970) carrying the same exceptions as referred to in the footnote, subsumed under article 2 of the European Convention on Mutual Assistance (April 20, 1959) where some Parties have reserved the right to co-operate in case of double jeopardy or where the offence is already under investigation in the requested State.[29] In addition, the European Convention on Transfer of criminal proceedings in criminal matters (May 15, 1972) provides in its article 3 for the possibility to waive or desist from proceedings if the suspect is or will be prosecuted

[26] PC/S/CP (2009) 4.
[27] Status as of December 12, 2008 (http://conventions.coe.int).
[28] Note however some exceptions in paragraph 3 of the amended article 2.
[29] See list of reservations http://concentions.coe.int.

by another Contracting Party. This decision is provisional if the final decision for prosecution has not been taken at the time of the request.

69. Apart from the multilateral Council-of-Europe Conventions, bilateral treaties may be in force between member States of the Council of Europe or between Council-of Member States and third Parties that may include the aforementioned principles. Since those treaties may not be ratified by all Council of Europe Member States it has to be taken into account that the overall system of *ne bis in idem* is not necessarily without gaps. It would, however, go too far in the context of this report to prepare an inventory about all possible interstate relations where it comes to the realisation of the principle of *ne bis in idem.*

70. The most frequently found text in the Conventional Articles are the wordings *the (same) offence*. In the practise of international co-operation – in particular extradition - this is understood as referring to the underlying conduct and not to the text and elements of the applicable offence or offences. On the other hand, the question if the same conduct is at stake, becomes more difficult to answer according as the conduct becomes more complex or involves more specific aspects.

71. As a demonstration of a different approach may serve preliminary decisions of the European Court of Justice of September 2006[30] concerning the *ne bis in idem* principle as incorporated in articles 54 to 58 of the European Union CISA.[31] The criterion to be applied by the Court are the wordings "the same act".
The leading case is the case of Van Esbroeck.[32] Van Esbroeck was convicted by a Norwegian Court because importing narcotic drugs into Norway. After having served his sentence partially he was released conditionally and returned to Belgium. There he was prosecuted for exporting the same narcotic drugs. The defendant appealed to article 54 CISA and for that reason the Belgium Supreme Court asked for a preliminary ruling of the Court of Justice. The Court rules that it is irrelevant that the CISA was not in force in both Contracting Parties concerned at the time of the commission of the crime. Relevant is only that it is in force at the moment of the second prosecution (i.e. in Belgium). Further answering the question whether the import in Norway and the export from Belgium of the same narcotic drugs should be considered as the same fact in the meaning of article 54, the Court considered that the wordings *the same acts* should be interpreted as the existence of a set of facts which are inextricably linked together, irrespective of the legal classification given to them or the legal interest protected. It is the task of the national court to make the definitive assessment whether this is indeed the case.
In the case of van Straaten *v.* the Netherlands[33] the person concerned was prosecuted in the Netherland for having imported a quantity of about one kilogram of heroine into the Netherlands. The Dutch court decided that the presented evidence was not convincing and acquitted the defendant (but convicted him for other relating charges). A couple of years later, the defendant was prosecuted in Italy for the possession and exporting of about five kilo's heroine and convicted *in absentia*. There was no doubt that the quantity heroine imported in the Netherlands made part of the quantity possessed and exported in Italy. The defendant claimed that the prosecution and conviction in Italy should not have taken place because of the prohibition in article 54 CISA.
The Court reiterates its van Esbroeck-criterion and concludes that it was not required that the quantities of drugs involved were the same or that the persons engaged in the act were identical, neither should exporting from a country be considered as a different act than importing the same drug into another country.

[30] C-150/05, Van Straaten v. the Netherlands and Italy, http://curia.europa.eu
[31] Convention on Implementation of the Schengen Agreement of June 14, 1985.
[32] Case C-436/04, Judgement of 9 March 2006.
[33] Case C-150/05, Judgement of 28 September 2006.

In the Casparine case[34], one of the preliminary questions of a Spanish court was if the marketing of goods in another EU-member States had to be considered as the same acts in the meaning of article 54 CISA if the defendant was prosecuted in Spain for the illegal importing of those goods but was acquitted because the prosecution was time-barred under national law. The Court sees by reiterating its van Esbroeck-criterion - the possibility that these acts may be considered as the same but leaves the final assessment to the national court.
The Court further finds that the one who profits from article 54 is the defendant who has been on trial finally disposed of in the Contracting State.

In the case Kraaijenbrink *v* Belgium[35] the defendant was prosecuted and convicted for the receiving and handling the proceeds of drug trafficking. A couple of years later the defendant was prosecuted in Belgium for the laundering of money, obviously obtained from the criminal acts for which the defendant was convicted by a Dutch court. The Belgium Supreme put a number of questions for preliminary ruling on the matter before the Court of Justice that decided as follows on the interpretation of article 54 CISA. The Court invokes its van Esbroeck-criterion but makes some reservation. In this particular case the acts are not the same acts just because they are linked together with the same criminal intention, but it is to decide by the national court whether the degree of identity and connection between all the facts to be compared is such that it is possible to find that the constitute "the same acts "in the meaning of article 54 CISA.

On the same date the Court ruled in the case of Kretzinger.[36] The person concerned was arrested when transporting a large quantity of tobacco by lorry into Italy without reporting to customs. The final destination of the tobacco was the United Kingdom. Kretzinger was released after questioning and acquitted in first instance but after appeal by the prosecution service he was convicted in absentia. He was arrested a second time with another cargo of smuggled tobacco at the Italian border but released and went to Germany. In Italy he was a second time convicted in absentia. Then charges were brought to Kretzinger before a German Court for smuggling the amounts of tobacco – for which he was convicted in absentia before an Italian Code - into Greece, which is a criminal act according to German Tax Law. In appeal, the Bundesgerichtshof would like to hear the interpretation of article 54 CISA.
The court reiterates its van Esbroeck-criterion. In this particular case, the Court says that the *conduct* of the defendant seems to be covered by the *same facts* because his intention was from the outset to transport the tobacco to the United Kingdom after taking possession of it and passing it through different Contracting States. A final assessment whether the conduct refers 'to the same acts' has to be made by the national court.[37]

This approach certainly enables to eliminate the number of jurisdiction claims that e.g. are directed against minor or subsequent elements of the criminal scheme act but it does ignores the ratio and specificities of the relevant national criminal provisions that were the reason why that State wants to assert jurisdiction. The ´same act´ approach may keep States - by launching a prosecution - from defending particular national or individual interests that are the rationale or even elements of the relevant national law that cannot or will not be taken

[34] Case C-467/04, Judgement of 28 September 2006.
[35] Case C-367/05, Judgement of 18 July 2007.
[36] Case C-288/05, Judgement of 18 July 2007.
[37] In addition the case of Klaus Bourquain, case C-297/07, judgment of December 11, 2008, could be mentioned that rules that a conviction given in absentia in one Contracting State and that by virtue of the laws of that State can no longer be enforced after a lapse of time stands in the way of a prosecution for the same facts in another Contracting State. The Court holds that it does.

into account if a prosecution is undertaken by another Party. E.g. if a person has – by means of the same tool or instrument – has hacked into a number of computer systems, this conduct in the Parties concerned could be subsumed under different criminal offences. In one State it could be considered as mere hacking of a system, in another State it could be considered as interference with a protected computer system. The 'same act' approach would ignore the different interests of the involved Parties. The 'same acts' requires full confidence in the criminal justice system of other Parties to the Convention concerned.

73. Conclusions

1. Application of the traditional principles of jurisdiction in the field of cybercrime may lead to a growth of concurring jurisdiction claims. National courts show some reserve to assert jurisdiction in cases of information made available on websites and comparable facilities. Formal restrictions (mutual co-operation) and pragmatic considerations may restrict the number of actual concurring jurisdiction claims.
There is a trend that a cyber crime case does not consist of a single crime but usually it is a complex set not only of crimes in the sense of the Cybercrime Convention but also involving other cyber crimes as well as traditional crimes. Setting rules on – restricting – extraterritorial jurisdiction therefore should not be undertaken within the frame of cybercrime. Where it touches upon general issues of international law, the Council of Europe can only contribute to a possible solution of the problem...

2. Although the traditional factors to prioritise jurisdiction claims seem to have lost some sharpness in the internet and in the cybercrime scene, a mechanism of prioritising jurisdiction claims is feasible. It is in the line of the function of and the position of the CDPC if it would take the role of mediator between Parties to the Cybercrime in jurisdiction cases. It is important that the CDPC is enabled to collect information on the matter. To this end the relevant provisions of the Cybercrime Convention should be amended. In relation thereto some inspiration may be taken from the European Union.[38]

3. The risk of concurring jurisdictions may affect the position of the suspect. Transnational regulation of *ne bis in idem* therefore is recommendable. Although cybercrime has a role in it, this problem is a consequence of increased international interaction in which the internet is only one of the instruments. Application of a "same acts" approach carries the risk of oversimplification. Use could be made of the experience regarding the European Union Green Book on this matter[39], taking into account that unlike the CDPC institutions like Eurojust and Europol have a more 'natural' bond with the law enforcement authorities of Member States.

4. In the fields of cybercrime co-operation is often between law enforcement authorities of different States. It is recommendable that as part of this co-operation a decision is taken about a possible transfer of the case to the most appropriate jurisdiction. A problem is that the relevant CoE instrument in place is limitedly supported by the Member States and no other States are Party to this Convention. It

[38] On the basis of the recently agreed reform of the Eurojust- regulation[38] Eurojust is entitled under article 7 (2) to provide a non-binding opinion on how a jurisdiction conflict between two or more EU-member States should be settled. If a Member State does not accept this opinion it has to explain and provide his arguments. This may help to analyse – somewhere in 2009 or later – if legislation would be necessary and if a mandatory list of criteria and a standard procedure to allocate jurisdiction are needed.

[39] Green Paper, On Conflicts of Jurisdiction and the Principle of *ne bis in idem* in Criminal Proceedings (COM 2005/698/FINAL).

is nevertheless to review this instrument or, as a first step, introduce it a basic version in the Cybercrime Convention.

6 Jurisdiction to enforce

74. There is little need to study in this section classical cases of the execution of extraterritorial jurisdiction to enforce that were accepted or not-disputed under public international law. Usually those cases refer to extreme circumstances such as war or similar common danger and should not be brought into connection with ordinary cyber crime or ordinary internet traffic. Conflicts of jurisdiction often concern executive jurisdiction. In this area limitations imposed by international law are clearer than in the area of legislative or judicial jurisdiction.[40]

75. As to the Cybercrime Convention the drafting group was fully aware of the volatile nature of data that is processed, stored and transferred on the internet the need was recognised that law enforcement authorities of one State should avail over means to obtain such data before it is lost. The result of the discussions was the drafting of article 32 that allowed unilateral transborder activity in a very limited number of cases. The conclusion therefore was that in other situations a formal request for mutual assistance should be done. In addition a number of provisions in the Cybercrime Convention seeks to expedite the procedure and provides for preliminary retention of the data sought in order to prevent it loss or modification in awaiting of the formal procedure of letters rogatory for its disclosure.

76. A leading consideration to debate regulation of trans-border searches was that international communication networks like internet easily enable to execute trans-border investigating activity and that law enforcement authorities, in the course of an investigation, are not always aware and able to establish that a search extends to computer systems and data located in territories of other States. Explicit international regulation of the possibility of trans-border searches and international agreement about conditions therefore should be preferred over a *laisser-faire* or adherence to the questionable hypothesis that State Parties in all circumstances strictly limit the scope of their criminal investigations in electronic networks to the reach of jurisdiction to enforce reaches under public international law.
In order to appreciate the system of international co-operation as embodied in the Cyber Crime Convention, particular attention should be paid to what has been posed in Council of Minister's Recommendation 95 (13) about the feasibility of trans-border network searches, the reference to such trans-border activity in the terms of reference for the drafting of the Cybercrime Convention and about the reference to mutual assistance as the designated means for international co-operation in the Explanatory Memorandum.
The Recommendation reflects the common understanding of the drafters that investigative activity of law enforcement authorities of a State Party in international communication networks or in computer systems located in the territory of another state may amount to a violation of territorial sovereignty of the state concerned, and therefore cannot be undertaken without prior consent of the State concerned.[41] Such activity may imply the use of data processing capacity or affect data stored in computer systems that fall under the territorial jurisdiction of that State. At this point, it is uncertain if State Parties indeed would consider trans-border activity in by means of international communication networks as a violation of territorial sovereignty.[42]

[40] European Committee on Crime Problems, Extraterritorial criminal jurisdiction, Strasbourg 1990, p. 18.
[41] Problems of criminal procedural law connected with information technology, Recommendation R (95) 13, paragraph 80 and 157.
[42] See for different positions UNAFEI, The Global Challenge of High-tech Crime, Tokyo 2001, paragraph 63, p. 16.

77. The principle rule of international law still can be found in the Lotus-decision of 1927 that is based on a strict interpretation of territorial sovereignty. In essence, this interpretation has been upheld where it comes to physical presence and activity of State representatives on the territory of another State without permission of the competent authorities of that State. Where in these modern times, investigative activities can be undertaken within the territory of another State by means of international communication infrastructures – without physical presence on the territory of other States, the question is how the principle rule of the Lotus case has to be interpreted in these situations? Should the access of a computer system or data located in another state by domestic law enforcement authorities without prior consent of the competent authorities of the State be considered as a violation of territorial sovereignty? Would it be different in case of an electronic communication between a domestic law enforcement officer and a person present on the territory of another State in order to obtain information of evidence? In the line of the Lotus-case one would assume that such actions require permission of the State concerned. Considering the nature and use of international electronic communication structures or other technological facilities a more pragmatic approach could be defended.

78. Recommendation 95 (13) leaves it to individual states to negotiate the circumstances under which they mutually permit each other to carry out trans-border searches. Trans-border network searches could, however, be an important means to secure vulnerable data that may be lost due to time-consuming formalities of mutual assistance.
The terms of reference of the Cybercrime Convention aim at further regulation in the Convention concerning the latter issue, indicated as "trans-border network search". The drafting committee examined seriously under which conditions and according to which procedures Parties to the Convention would allow each other such trans-border investigative activity, taking into account the rights of the defence of the suspect and third party interest.[43]

79. When drafting Article 32 several examples of possible trans-border investigative activity were considered but finally the common understanding of the negotiating Parties remained restricted to what is now formulated in *litera* a and b of the article.[44] It was concluded that the time for an overall regulation of "trans-border network searches" had not yet come and the need for such a complicated regulation had to be established on the basis of experiences with the present instruments. Given the fact that self-help of national law enforcement authorities through trans-border network searches was not to be made legally possible, the mutual assistance facilities of the Convention were based on the classical international regulation, be it that specific powers and procedures were drafted because of the vulnerability of electronic evidence and the need to keep it available independent of the time that is involved with the formalities of mutual assistance requests. In other words, if a Party would need electronic (evidentiary) material that is being processed, stored or transferred by a computer system located in territory of another Party, the former Party should apply the procedures of mutual assistance provided for in Chapter IV - or if applicable under other international agreements in force between the Parties concerned. The former Party is also entitled to apply art. 32, if this would render a satisfactory result as well.

80. Law enforcement should fully act within the scope of the authority of the person concerned and not exceed it. The person concerned who enables access finds himself within the territory of the investigating Party. Data under his control may be accessed by law enforcement authorities of that Party only if this person *voluntarily* consents that law enforcement authorities access to data to which he is legally authorised. The fact that this person is authorised to access and possibly manage this data does not imply that other

[43] Explanatory Memorandum, paragraph 11, item iv.
[44] The issue was also systematically debated within the frame of the G8 Action Plan.

(legal) persons are not authorised to access or manage the same data. The person concerned is entitled to refuse co-operation if the intended action of law enforcement would exceed or threaten to exceed the scope of his authority. It is not to be tested by law enforcement authorities if co-operation is refused on proper or valid grounds. Refusal means that article 32 (b) is not an option and therefore the route of mutual assistance will have to be followed.

81. The person who co-operates with law enforcement authorities in the case of art. 32 (b) is present in the territory of investigating Party and is therefore subject to the law of that State. Art. 32 (b) cannot be used to obtain co-operation of a person that does not fall under the jurisdiction of the investigating State. In the latter case, to avail over evidentiary material held by a person present at the territory of another State Party, mutual assistance procedures should be applied. If and how a mutual assistance request is executed, is up to the requested Party on the basis of its domestic law, applicable to persons under its jurisdiction.

82. Paragraph 294 of the Explanatory Memorandum does not provide for precise criteria in order to determine when a person is legally authorised. This authority may have a basis in the law – civil, administrative or even criminal law – or in other regulations. In most cases authorisation will have been established on the basis of a contract. Article 32 (b) does not make a distinction whether this authority is derived from domestic legal sources or contracts or has a legal basis connected with the Party where the data intended to be accessed are located. The person concerned may refuse to co-operate if he esteems that this would exceed the scope of his authority, whatever the legal basis or source. Article 32 (b) does not regulate the manner how the voluntary consent of the person concerned should be obtained. Although article 32 (b) does not say so, the consent must be obtained prior to the access to the data concerned and I would add that the consent must be given explicitly and well-informed. If these (legal) persons would reside on the territory of another State there are some limitations. The action of law enforcement authorities obtain voluntary consent would already be considered by some States as a prohibited interference with domestic affairs.

83. The relevant question here is, if the technological environment and the use being made of it is still the same as at the time of the development of the Cybercrime Convention. The answer must be no for several reasons. This is not a technological report but some factors have to taken into account. In a general sense it can be said that it has become extremely complicated to trace a criminal and his activities in the internet. One reason is the abundant choice of communication networks and means of communication - think of mobile equipment and VoIP - the systematic application of encryption (Skype, certain types of communication equipment) at random, the existence of software that may conceal the route of a communication path and the need to act really expeditedly if a trace or a source of communication needs to be established. It is true that an IP-address may refer to a certain service provider and thereby to the territory of a particular State. Finding an IP-address does not mean that the investigation of the source or destination of the communication is concluded, because an IP-address may not adequately identify the person involved in the communication. In particular, problems may occur if the communication is transmitted through other ISP's and servers. The agreed preliminary measures under the Cybercrime Convention, although already more flexible and less time consuming than in traditional mutual assistance relations, will cost time, and time is the decisive factor in safeguarding volatile data, in particular if the exact location of the server in question is not known or can only be identified through time-consuming efforts, that will come too late.

84. On the internet open source is software available, called TOR, short for The Onion Routing[45], that is directed against the analysis of traffic by a third party, including law enforcement authorities. A communication is sent through relays operated by volunteers all over the world, causing that it is not possible to find out which sites have been addressed and vice versa that visited sites cannot see the source of the communication. The principle idea is that the communication between source and the destination (the site) is lead over as many anonymous servers. Identification of the source is that situation not directly possible unless one would take the time and the effort to follow and analyse all the individual steps in the communication. The system was developed for military purposes (US Marine) to conceal the position of ships.
In a German child porn case some TOR-servers were seized in September 2008 being the exit-nodes of the TOR-onion. No further action against the servers was taken. Probably the seizure did not bring the investigation further.[46]
A similar application is Freenet, particular in a peer/to/peer/environment.[47]

85. Both features are applied to conceal the chain of communication to protect freedom of expression against government control. This is not the place to discuss the scope of freedom of expression. Around the globe different standards exist about the scope of freedom of expression even between countries that support international human rights instruments. At the same time it is clear that such technical facilities may be misused to circumvent criminal liability, not only in cases of freedom of expression.

86. From law enforcement practice cases are known that criminal activity is otherwise moving from one IP address to another and that for example use is made of virtual hard disks or other temporarily storage facilities. The communication between the related persons takes place by means of storing text files at this hard disk and are deleted after the other party has read the message. A request to issue a preservation order will only safeguard the situation at the virtual disk at a certain moment of time after the request has been done and will not secure the whole communication. A request for surveillance, if permissible at all, costs time and may not render result. It is my personal impression that this situation is experienced more and more, although I do not avail over adequately documented cases that will demonstrate the seriousness of the problem for criminal investigations. In this case the preliminary measures of the Cybercrime Convention, although a major step forward international co-operation, are of a too limited scope and are not always appropriate.

87. In both cases illustrated, the choice seems to be to go the way of mutual assistance, provided that the appropriate jurisdiction or jurisdictions can be established or to safeguard the information that is at hand at the time of the surveillance, even if this would imply unilateral cross border action. It is therefore recommendable to further explore the cases and circumstances under which such unilateral actions could be agreed upon amongst the Parties to the Cybercrime Convention while preserving the rights of the defence and of third persons.

88. It is not always possible to immediately determine the physical location of data in the internet. Data are moving and being moved over the internet. In particular, where the person who is in control of data moves that database frequently from one server or proxyserver to another, electronic surveillance of his activities will only reveal that the person concerned logs in into that database and will only (partly) disclose the content of that database in as far as it is included in the intercepted (IP-) communication. Suppose that the person concerned is suspected of an internet scam or other criminal activity. The content of

[45] http://www.torproject.org/index.html.en
[46] http://news.cnet.com/8301-13739_3-9779225-46.html
[47] http://freenetproject.org

the database, therefore, would reveal his already committed and possibly planned criminal activity. By IP-interception it is only possible to establish that there is contact between the suspect and the database, it is not possible to be sure about the exact physical location of the data. The suspect is not only capable of changing his IP-addresses, it is also possible to move the database within seconds from one server of proxyserver to another. If access to the data base is necessary to obtain evidence of criminal activity the suspect, it will hardly be possible to take legal action around the internet, because there is no certainty whatsoever of the physical location of the data, necessary as a nexus for the execution of investigative powers within the domestic sphere or *a fortiori* within the international sphere.

89. The result of the negotiations of the Cybercrime Convention was that transborder investigative activity was not accepted in principle. Instead, system of expedited mutual assistance combined with preliminary measures was chosen. Today, cases are known where internet users exchange information by means of temporary files or disks, whereby the information does only exist for a very limited period of time at least in such a way that possible traces are deleted before a request through the 24/7 contact point for preservation can be made or be carried out. For regular traffic or ISP-involvement, the 24/7 system may remain adequate and appropriate. I do not avail over information, on how frequent these cases referred to above occur or whether this would mean an insurmountable problem for the investigation of (serious) cases. For this and other reasons some Parties[48] have enacted a penetration power, i.e. a power to access other computer systems in order to copy data from those systems or in order to install spyware to be informed about the activities undertaken by those systems.

90. Before taking decisions, it should be extensively documented and analysed if there is indeed a need for direct transborder access to data and data flows where other measures are not adequate or fail. This need could be explored by a technical committee that operates under the responsibility of the T-CY.

[48] See Belgium.