15th BILETA Conference: "ELECTRONIC DATASETS AND ACCESS TO LEGAL INFORMATION".

Friday 14th April 2000.
University of Warwick, Coventry, England.

Reflections on Enforcement Measures and Penalty Levels in Computer Misuse Legislation: The Council of Europe Convention on Crime in Cyberspace

Indira Carr* and Katherine S Williams**

*Reader in International Commercial Law, University of Kent, Canterbury, UK;
University Fellow, University of Exeter, UK;
Special Lecturer, University of Nottingham, UK.
**Lecturer in Law, University of Wales, Aberystwyth, UK.

INTRODUCTION

Since 1997 the Council of Europe has been working on an international instrument to fight Internet crime, the Draft Convention was set to be published in December 1999. The intended focus of this paper was this Draft Convention on Cybercrime. The paper would have analysed the framework of the Convention in general and examined various provisions dealing with child pornography, illegal accessing of computer networks, and cross border investigations. Unfortunately the Draft Convention has not been published and is not now expected until December 2000. Despite this rather serious lacuna we have gathered as much information as we can and shifted focus a little so we hope to offer an equally interesting consideration of the need to intervene in this area and some tentative consideration of the possible contents of any future Convention, if it ever sees the light of day. This is very much a work in progress, we wish to retain copyright on the material and ask delegates to respect that these are not our final comments on the work.

The exponential growth in the use of computers and of computer technology is clear as is the seemingly relentless growth in electronic trading around the world and the ever more ingenious uses to which computers are put, both acceptable and unacceptable.[1] http://www.cert.org/research/JHThesis/start.htm[l] The economic potential of devices such as e-commerce[2] and the importance of encouraging a flourishing market in all aspects of this technology has been fairly central to national governments[3], regional groupings[4] http:///www/cordis/lu/esprit/src/ecomcom.ht[m], chambers of commerce[5], trading associations and international organisations.[6] In an attempt to secure the investment which will follow this industry governments seem to compete to provide the most advantageous legal environment in which to facilitate the potential wealth creating aspects of IT.[7] http://www.whitehouse.gov/WH/New/Commerce/about.htm[l]http://www.doe.gov.in/it-bill.ht[m]

Regional groupings and bodies have also been busy.[8]http://www.la.warwick.ac.uk/jilt/98-[3] The other aspect which seems to be perceived as necessary to economic strength in IT is to curtail those aspects of the use of the technology that threaten or may undermine its use, either because of customer insecurity or because of any possible unacceptable threats to the business interests concerned.[9]http://www.usdoj.gov/criminal/cybercrime.juvenilepld.ht[m] Therefore securing this electronic environment from intrusion continues to be an issue[10] and even those at the cutting edge of e-commerce and of the technology, the largest and supposedly most secure systems are not immune.[11] So far as e-commerce is concerned protection from some of these threats could be tackled through technological innovation (encryption and other devices[12]), through insurance and through criminal legislation. Many individual governments (e.g. the US, Singapore, the UK, Malaysia, many European states, soon India)[13] have specific legislation criminalising intrusive and destructive activities directed at computers, some control other uses of computers, or are discussing such measures. As each state legislates for perceived misuse of the technology they seem to compete to prove that they provide the most secure environment within which to locate an IT business. Given the borderless nature of computer crime one cannot but wonder whether the different approaches might create a `haven for computer criminals'.[14] Such a scenario would be destructive for all e-commerce and other computer industries as no matter how secure the state within which they operate they will always face the danger of falling pray to someone working from another state, or possibly even to another state wishing to commit commercial sabotage. Within this environment what might be far more useful is international standards which should be met by all states. One such blueprint is the basis of the intended Council of Europe Draft Convention on Cybercrime.

Before turning to a consideration of the possible sphere of such a Convention it might be useful to explore the terminology. The phrase `computer crime' or `computer misuse' (IT crime and cyber crime) has no precise definition and tends to cover a multitude of computer related offences[15] ranging from unauthorised access to computers and computer held material, causing damage to computer held information, trafficking in computer passwords and `hacking-friendly technology', [16] manufacturing/selling pirated copies of software[17] through to production and distribution of computer generated information/sexual images of minors. Few countries have legislation broad enough to criminalise all types of computer crime[18]http://www.ncis.co.uk/newpage1.ht[m] though new proposed legislation in India would come close to this.[19]http://www.doe.gov.in/it-bill.ht[m] We will test how far the discussions in the Council of Europe seem to be moving in this direction.

THE COUNCIL OF EUROPE CONVENTION ON CRIME IN CYBERSPACE

BACKGROUND

Computer misuse, be it hacking, distribution of offensive material, or electronic message forging is not subject to geographical containment. The attempt on the part of countries that have legislation has been largely piecemeal. Legislators, politicians law enforcement officers and the wider public are of the opinion that harmonisation of the laws would be one way of ensuring that all countries have the choice of adopting a legislation that gives a minimum level of protection from mischief mongers.

The Council of Europe in 1997 took on the task of drafting an international instrument to fight Internet crime.[20]http://www.coe.fr/europa40/e/9704/internat.ht[m] It has not been possible for us to obtain current documentation. However on the basis of the information received it is possible to say something about the broad framework of the proposed Convention.

FRAMEWORK

It seems that within the general the framework of the Convention the areas to be covered are likely to include:

* Definitional articles

* Measures at a National Level

- Substantive criminal law

- Procedural law

- Jurisdiction

* International Co-operation

- Principles

- Provisional Measures

- Extradition

- Mutual Legal Assistance - general and actual measures

- Channels of communication

- Other provisions

- Form and content of requests and notification

* Final Provisions - largely the operation and administration of the Convention.

CONTENT

Definition

Given the rapidity of advances in information technology any legislator faces the difficult task of defining computer system. It seems that the Council of Europe may be considering a definition linked to the function of data processing enabling the definition to include telecommunications systems and also permitting built in room for the inclusion of future advances in this science.

Measures at a National Level

Substantive criminal law

The Offences

As for the substantive criminal law provisions it seems that the Convention will be recommending that parties to the Convention put the following broad categories of criminal offences in place:

1. Offences against the confidentiality, integrity and availability of computer data and systems (to include unauthorised illegal access to a computer system, illegal interception encompassing eavesdropping, blocking or interfering with the use of a system, import/sale/distribution of devices capable of commission of the offences against the confidentiality or integrity of a computer system or data);

2. Computer related offences (namely, computer forgery and computer fraud)[21];

3. Copyright related offences (infringement of copyright as defined in the Berne Convention for the Protection of Literary and Artistic Works 1886, the WIPO Copyright Treaty 1996, and the 1993 TRIPS Agreement involving a computer system);

4. Content related offences. It seems that this will involve some harmonisation of laws relating to child pornography through the medium of a computer. It might also require states to ensure that other criminal offences under its normal laws that relate to the content of the information (such as e.g. those involving racial hatred or pornography other than involving children) will apply when the conduct is committed through the means of a computer.

The offences in the first three categories make their appearance also in the Council of Europe Recommendation R 89(9) on Computer Related Crime.[22] Category 4 is an important development in the light of the use of the Internet for distribution of offensive material. All of these except the final part of category 4 would involve harmonisation of national laws concerning the areas discussed. Clearly such harmonisation will facilitate agreement on and application of other aspects of the Convention, particularly those which relate to co-operation on matters such as enforcement (transboarder searches etc.). It is the lack of any attempt to harmonise the final aspect of the fourth category, other content based criminal laws, which may cause conflict over the inclusion of broad powers in relation to this within the Convention. As will be seen the Convention foresees a fairly high level of co-operation at the enforcement stage and this will be much more difficult to obtain for an offence that is not recognised in one of the states necessary to a satisfactory investigation. Inclusion of these other content based crimes may therefore cause the co-operation in enforcement sections to be watered down which might undermine one of the strengths in this international approach.

Once the offences are finalised the Council of Europe it will decide which to which offences the provision on `attempt' should apply. The suggestion is that there may be some offences to which this is inappropriate. Aiding and abetting any of the offences is expected to be made a criminal offence. The Convention will harmonise the meaning of these concepts and importantly it is expected that aiding and abetting will take on a very wide meaning, including instigators and accessories. This will catch within the criminal net many people who are caught on the periphery of an offence, many who are not included within present criminal laws within nation states.

Corporate Liability

Importantly the Convention will ensure that legal persons will be held liable for any of the above criminal offences committed for their benefit, even if they do not actually benefit. The limiting factor is that they will only be liable for the actions of key personnel within their organisation, or those ordered by such key personnel even if carried out by others. The need to ensure that it is possible to trace the infringement back to those who are responsible at the decision making level of the institution is very clear, otherwise any disgruntled employee might be able to commit offences and cause the company to fall foul of the law. With this inclusion it will be possible to try to prevent industrial espionage, a factor which may prove essential to economic stability. Of course there may be problems with the provisions concerning enforcement and co-operation between states where one state is asked for search powers against a large and economically strategic company situated within its territory. This is likely to be exacerbated where the request comes from another state where the supposed victim is a direct competitor of the first company. Inclusion of this may therefore limit the lengths to which states are willing to agree to broad powers of co-operation on matters involving investigation.

Penalties

The Convention requires that the Parties signing the Convention should take steps to adopt a penalty scheme that is proportional and dissuasive. It does not suggest a scheme or scale leaving it to the

State concerned to deal with the issue according to their principles of criminal justice. Nor does it suggest that there should be any attempt to ensure proportionality as between member states as to the penalties imposed so that presumably the proportionality here refers purely to scales adopted within each state. This may prove to be a weakness of the Convention, as we have discussed elsewhere[23] states wishing to attract economic inward investment may be tempted to compete with each other to be the most punitive on this type of offence and therefore the safest in which to locate. Despite the fact that such an approach is illogical when dealing with such a technology which does not respect international boundaries and with a transboarder business structure there are indications that this is already happening therefore some harmonisation of this area might have proved useful to the success of the Convention in dealing with such an international problem. On the information we have there has not yet been any decision concerning the status of Internet Service Providers (ISP). In discussions the issues concerning the protection of personal data and the problems this would cause were ISP liable for all materials posted were considered at length but so far as we are aware these have not yet been resolved. At the time when this was being discussed it was noted that the EU were then in discussions concerning a directive on the operation of ISPs and that therefore one should delay until these issues had been more fully considered in that forum.[24]

Procedural law

The area of enforcement is possibly the most complex and controversial of the Convention. New technologies have brought with the new possibilities in policing, particularly in investigative techniques. Whereas in the past searches were purely physical and any extraterritorial activity was easy to spot and prevent with modern technologies this is no longer the case. Virtual searches are becoming increasingly used in many criminal investigations and these along with interception of telecommunications know no territorial boundaries. These investigative techniques can therefore have consequences in other jurisdictions, the consequences may be either intentional or inadvertent but the extraterritorial aspect is the same and needs to be recognised and possibly also legally regulated. At the moment these investigative techniques are not effectively dealt with at n international level. The G8 did agree that access to computer data where there was an extraterritorial aspect should only occur where there is mutual legal assistance from within the state or where the person with authority over the data consents but this is a limited answer and has not solved the problem. The difficulty is that some states believe that, as there is no physical territorial presence and as one cannot be sure where a search will lead that one should merely be permitted to access data from anywhere as long as it is done through the domestic authorities. Whilst other states are of the opinion that a request to the state in which the search is to be made should always be forthcoming before any search takes place, and that state should always be allowed to refuse such a request. The main move seems to be to require consent and, where data is accessed from another jurisdiction in error, possibly whilst searching a private computer, to seal that information (not to use it or analyse it) until consent is obtained. However it is envisaged that states will be obliged to preserve information to ensure that it does not get destroyed or tampered with until such consent is applied for and either obtained or denied. There is also some discussion of a need to give reasons for any refusal and an assumption that such a position will not be adopted unless necessary to protect certain important rights within the requested state. These sections and the co-operation which they envisage seem likely to give rise to considerable discussion and negotiation, we suspect that it is here that most changes are likely between now and next December. They are discussed again in the section on co-operation, as within this area there is some duplication within the proposed Convention. In the final draft it seems likely that the sections concerned with co-operation on powers of investigation will appear separately under the heading *Procedural Law* whereas all other aspects of co-operation, especially the general and broad underlying principles on co-operation which are intended to give the real power to all the rest of these articles, will appear later under the heading *International Co-operation*.

Jurisdiction

The Convention seems likely to embrace a fairly broad jurisdictional approach largely to ensure that activities deemed criminal under its definitions are prevented and enforced.

International Co-operation

There is a separate Chapter on international co-operation, which undoubtedly is of central importance for controlling computer abuse. The Convention includes provisions that require the Parties to co-operate on the basis of existing international agreements or bi-lateral agreements on co-operation in criminal matters. In their absence or if the provisions are less favourable than those in the Convention,[25] the latter will come into operation. The Convention expects that the Parties will give the widest possible assistance by the speedy processing of requests for information necessary for investigation purposes. It also expects states to adopt legislative measures that will enable them to comply with requests for searching computers, seizure of data, preservation of data etc.[26] Since preservation of the data will be vital for prosecuting purposes the Convention is likely to include provisions on the preservation of the data and the extent to which a request for preservation will be met, it is expected that consent to preserving data will almost be a formality. The criminal offences listed in the Convention will be extraditable offences.

Of course, a problem that will need to be addressed is who will bear the costs that will be incurred where co-operation is required at an international level? It will be interesting to see whether the Convention will provide any formula for cost allocation.

CONCLUSION

Almost all states or groups of states competing internationally and in modern economic markets want to provide both the physical and legal environment in which the use of IT in the commercial sphere is encouraged and supported. In the face of this fierce competitive environment the use of law to control activities that damage or have the potential of damaging business is important. Part of the necessary protection is believed to be the control of unacceptable uses of computers.[27] Strict criminal laws, wide powers of enforcement and harsh penalties may all serve to make a state more attractive as a place to locate a large economic organisation whose business is heavily dependent on new technologies. However, competition is always in a state of flux and in order to maintain the competitive edge more and more harsh criminal laws and more intrusive enforcement measures may be passed. This might lead to a distortion in the general criminal laws within that state. All this is done with no evidence of any success.

It is our contention that national laws controlling computer security have served national interests rather than guaranteeing or providing greater security for computer users, whether they be individuals or companies. If criminal controls are to succeed then these need to apply across national boundaries, preferably have global application. Although a regional Convention has some merit in that it might harmonise laws over a number of national boundaries it also suffers from the same shortcomings as any national answer - different regional groups may compete market supremacy. Therefore although it is a move in the right direction it may not go far enough.

Having noted this major shortcoming the Convention would signal an advance - it harmonises criminal laws so facilitating agreement and co-operation in the area of investigative techniques. It seems that the Convention will be willing to tackle some of the more difficult issues such as corporate liability, co-operation on transnational enforcement. Unfortunately it has shied away from any indication of penalty levels, an area where national states may continue to compete and may thereby skew national principles on sentencing and criminal justice.

However misgivings about the use of the criminal law in this area remains. There seems to be some

concern that the presence of criminal laws may have led to false sense of security on the part of computer users so reducing calls for other, possibly more effective preventative measures from being developed or marketed. Alongside any criminal provisions there needs to be investment in research and development of innovative security measures and potential hackers might be usefully employed in such a venture. Insurance companies should be encouraged to increase their business in this area offering packages to both businesses and private individuals. One factor which may be reducing their effectiveness in this area is that the level of potential losses is very high and, as yet, possibly difficult to predict. States might sensibly consider ways in which this business might be encouraged, through taxation and / or other aid such as that offered to the insurance industry in the aftermath of the recent terrorist bombings in London. Insurance packages might sensibly require an organisation to install the most modern and effective security measures or at least set minimum requirements for a safe electronic environment. This would enhance security far more than any criminal law is ever likely to achieve.

One of the interesting features of the growth in technologies is that secure devises attached to hardware and software do not seem to have been developed as fast as other products. This looks odd. The clamour by businesses and individuals alike for more effective, often invasive security devises in the non-electronic environment (where the crime involves some sort of physical invasion of property or personal integrity) is very clear. In this area most of us are now loathed to rely on the criminal law and its enforcement to protect us and our property. Better locks, security devices such as burglar alarms and CCTV are all deployed to protect property (situational control). It seems that similar techniques are not necessarily as widely used to protect the electronic environment, even by businesses. Wider use of measures that alert businesses to unwanted visitors (the cyber equivalent of guard dogs) and employment of those with specialised knowledge of security breaches might make a significant difference and boost confidence in the e-commerce. It is arguable that the appearance of protection from hackers via the criminal law has slowed down the rate at which means of securing computer data has been developed. It may therefore have reduced rather than increased levels of security. If businesses continue to drag their feet in this way and the insurance market does not alter anything then an even more effective way or ensuring consumer protection would be for a state to set minimum standards of security to be met by companies, breach of these might lead to a criminal sanction. Enforcement might be along the lines of Health and Safety, the first intent being to secure compliance and therefore the enforcement authorities could give expert computer security advice and only use enforcement powers in the face of flagrant breaches. If this were done soft-ware houses might feel more pressure to add more sophisticated electronic safeguards as standard features in new products and businesses might require such facilities in all user dedicated software.

Criminal measures designed to deal with those who transgress computer integrity in an unacceptable manner are therefore only part of the answer. Putting such laws on an international footing is a move in the right direction and may secure greater compliance with acceptable codes of conduct in the use of new technologies. Reliance on these measures is however, only part of the answer and both businesses and states have to look more broadly at the problem is they are genuinely interested in arriving at solutions. There may be need for greater pressure on the IT industry to be more responsible in the research and development of security measures. This has been improved in recent years. There may also be mileage in the use of insurance and possibly or business regulations to ensure the use of security measures, especially to protect consumers in e-commerce, but possibly more widely.

---

[1] The number of Internet users is expected to be between 200 million and 2 billion users by 2000 - see John D Howard `An Analysis of Security Incidents on the Internet' available [). See Matthew Wall, `Internet shoppers spend, spend, spend']*The Sunday Times* (Business Section) August 29, 1999, p, 2.

[2] Electronic commerce is defined as trade that takes place over the Internet with a buyer visiting

the seller's website. It includes business-to-business (B2B); business-to-customer (B2C), consumer-to-business (C2B) and customer-to-customer (C2C) trade

[3] The British Government is vigorously promoting e-commerce and is putting pressure on computer retailers to cut hardware and software prices in order to fuel growth in e-commerce. British Telecommunications is also restructuring call charges to make net access cheaper (see Dominic Rushe & Claire Oldfield `E-Mania' *The Sunday Times*, Business Supplement, September 19, 1999, p, 5.) See also *The Times* special supplement `The Future of Business' November 23, 1999.

[4] The European response to electronic commerce is also to promote its vigorous growth, to provide a coherent policy framework for future Community action and to achieve a common European position. See *A European Initiative in Electronic Commerce* (COM (97)157) ([).

5] The ICC (International Chamber of Commerce) is currently working on Rules for Electronic Trade and Investment, as are many other organisations.

[6] UNCITRAL (United Nations Commission on International Trade Law), OECD (Organisation for Economic Co-operation and Development), the EU (European Union),have all been addressing the legal problems associated with electronic trading. See for instance, UNCITRAL Model Law on Electronic Commerce 1996, as amended 1998 (also A Brooke Overby ;Will Cyberlaw be Uniform? An Introduction to the UNCITRAL Model Law on Electronic Commerce' *Tulane Journal of International and Comparative Law* 1999 (7):21; R Hill & I Walden `The Draft Model Law for Electronic Commerce: Issues and Solutions' *Computer Law* 1996 (13:3):18.

[7] For example in the developed world the US Government has established a framework for Global Electronic Commerce which outlines the Administration's strategy for increased business and consumer confidence in the use of electronic networks for commerce. Details of the principles and other information can be found on [.

In the developing world the Indian Parliament is currently considering the Information Technology Bill 1999. The Bill is comprehensive including provisions on digital signatures, e-commerce and computer misuse ()

8] For example in the arena of digital signatures one finds the European Draft Directive *A Proposal for a European Parliament and Council Directive on a Common Framework for Electronic Signatures* (OJ 1999 C 325/04). See also in relation to the EU developments A Kelman `Just say "Non"' *Journal of Information Law & Technology* 1998 (available [); R Julià Barcelò & T C Vinje `Another Step Towards a Framework for Electronic Signatures: The Commission's Directive Proposal']*Computer Law & Security Report* 1998 (14:5):303. See also ` The UNCITRAL is currently discussing the Draft Uniform Rules on Electronic Signatures (Doc. A/CN.9/WG:IV/WP.84, 8th December 1999).

Whilst in the international recognition of electronic documents UNCITRAL adopted a *Model Law on Electronic Commerce* in 1996. This has already met with success. Singapore designed its Electronic Transactions Act 1998 around the Model Law. See Endeshaw, A `Singapore's Electronic Transactions Act 1998' in *Information and Communications Technology Law* for an appraisal of the legislation. Australia also has modelled its recently published Electronic Transactions Bill 1999 on the Model Law. The EU is currently considering a draft directive *A Proposal for a European Parliament and Council Directive on Certain Legal Aspects of Electronic Commerce in the Internal Market* (OJ 1999 C 30/04). See also D Church, M Pullen & Jk Winn `Recent Developments Regarding US and EU Regulation of Electronic Commerce' *International Lawyer* (1999 (33):347; J Dickie (1999) *Internet and Electronic Commerce Law in the European Union* Oxford: Hart Publishing.

[9] Hacker attacks are not confined to commercial sites. They are known to attack key installations servicing the community. For instance. in March 1997 vital services to the FAA (Federation Aviation Authority) Control tower servicing airports were disabled by a juvenile hacker for six hours. He also downloaded patient records from a pharmacy computer during his `hacking voyage' (see [). Information obtained in hacking may be put to more sinister uses - a British group of hackers are reported as having broken into the computer systems of multinational companies. VISA (one of the victims) has received a ransom note for £10 million. According Kershaw (]*The Sunday Times Magazine* `Lap Top Cops' January 16, 2000, p, 20) a US Government Report claims there will be 20 million people world-wide with skills to launch a cyber attack by 2001. The vulnerability of computer systems to external and internal threats (criminal acts, misuse for political purpose, acts of war, catastrophes such as flash-over in electrical cables and fires, security for sensitive/confidential information) was foreseen in the late 70s. See for instance, *The Vulnerability of the Computerized Society - Considerations and Proposals'* Report by a Swedish Government Committee (Sårbarhetskommiteé), 1979 (trs. John Hogg). The title in Swedish is "ADB och samhällets sårbarhet, övervaganden och forslag".

[10] see Roger Trapp `Security Breakthrough on the Internet' *The Independent on Sunday* Section 2, December 20, 1998, p,21. According to this news item TriStrata Security, based in California, has created a security system which uses the Vernam cipher regarded by cryptographers as "the world's only theoretically unbreakable encryption system". It is expected that the next big battle fought over the Internet will be encryption and particularly the extent to which policing authorities should have access to keys to decode encrypted information. Inevitably questions regarding rights to privacy and freedom of speech are raised.

[11] See the recent hacker (denial of service via an attack on a website with spoof traffic until there is overloading of the computer system) attacks on various websites such as amazon.com (top e-commerce web site), eBay (leading auction website) and CNN (news website) which serve to expose the dangers lurking in cyberspace

[12] Interestingly as the technology is created to enable more secure commercial use of computers, so its misuse by some who want to turn this technology to hiding their criminal activities is facilitated. States want to facilitate the potential of devices like encryption to facilitate wealth creation whilst preventing its use by criminals wishing to hide their activities, the balance is difficult - see the controversy over Part III of the Regulation of Investigative Powers Bill.

[13] For an account of computer misuse laws in Austria, Germany and other European countries see `Colloquium, Computer Crime and Other Crimes Against Information Technology' in *Rev. Int'l De Droit Penal* 1994 (64):1

[14] It is easy for those using computers to commit crime to cross national borders, to hide their real identity and whereabouts in a number of complex links and to vanish seemingly without trace. They might use data havens where there is no or little regulation of computer crime to hide their evidence or through which to route their communication links so as to avoid detection.

[15] According to Branscomb there are six motives where computers are subjects or objects of crime. These are (a) exhibition of technical prowess, (b) highlighting vulnerabilities of computer security systems (c) publishing or retaliating, (d) engaging in computer voyeurism, (e) asserting a philosophy of open access to computer systems and (e) sabotage. See A W Branscomb `Rogue Computer Program and Computer Rogues: Tailoring the Punishment to Fit the Crime' *Rutgers Computer and Technology Law Journal* 1990 (16):24. D S Wall in `Catching Cybercriminals' (*International Review of Law Computers & Technology* , 1998, 12(2), 201) posits four categories of cybercrime: cybertrespass, cybertheft, cyberobscenity and cyberviolence. Most jurisdictions seem to classify computer crimes into crimes where the computer is the object of the crime, where it is subject of the crime (such as in spreading viruses), and where it is an instrument of

the crime to commit traditional offences (such as fraud, blackmail). See M Wasik (1991) *Crime and the Computer* Oxford: Clarendon Press.

[16] see D Mann & M Sutton `Netcrime: More Change in the Organisation of Thieving' *British Journal of Criminology,* 1998 (38), 210.

[17] The Council of Europe's Recommendation R 89(9) on Computer-Related Crime for instance includes unauthorised reproduction of computer program within the minimum list of offences necessary for a criminal policy on legislation concerning computer-related crime (see p,55).

[18] See `Project Trawler: Crime on the Information Highways' which looks at the different types of computer crime and the laws that may be relevant to such crime. Project Trawler was launched by the National Criminal Intelligence Service (NCIS). It defines `computer crime; as an offence in which "a computer network is directly and significantly instrumental in the commission of the crime. Computer connectivity is the essential characteristic" (available[].

19] The Indian Parliament is currently considering the Information Technology Bill 1999. The Bill is comprehensive including provisions on digital signatures, e-commerce and computer misuse ([]

20] The Committee of Experts on Crime in Cyber-Space is charged with the responsibility of drafting the legislation (see []. The draft treaty was due by December 1999. Latest indications are that the Treaty will be made public in December 2000.

21] In 1997 the UN Manual on the Prevention and Control of Computer Crime estimated that 90% of economic crime (such as fraud or theft where a computer is used as the means of committing the offence) is committed by employees.

[22] The minimum list includes computer-related fraud, computer forgery, damage to computer data or programs, computer sabotage, unauthorised access, unauthorised interception, unauthorised reproduction of computer program and unauthorised reproduction of a topography. The optional list includes alteration of computer data, computer programs, computer espionage, unauthorised use of a computer and unauthorised use of a protected computer program.

[23] See Carr and Williams (2000) `A Step too Far in Controlling Computers?: The Singapore Computer Misuse (Amendment) Act 1998' *The International Journal of Law and Information Technology* 8(1):48.

[24] It is interesting to that in a civil matter on 29th March 2000 Demon Internet, a British Internet service provider, agreed to pay Laurence Godfrey 15,000 pounds plus legal costs (which could exceed 200,000 pounds) after it failed to remove defamatory material from a newsgroup it hosted.

[25] That is if the mutual legal assistance procedures and channels in the Convention are faster and easier.

[26] It seems that many of the Recommendations made in R95(13) are likely to find expression in the Convention. See I. Carr and K. S. Williams, (1998) `A Critical Analysis of the Council of Europe Approach to Harmonisation of Criminal Procedural Law Connected with Information Technology (Recommendation No. R95(13))'. *The Journal of Business Law* pp. 468-484. And P. Csonka (1996) *Information and Communications Technology Law*

[27] see, for example, the recent calls by the US and EU for urgent discussions following the hacker denial of service attacks referred to in footnote 11 (see `Clinton to Hold Internet Security Summit' *Wall Street Journal* February 11 2000; and The Associated Press February 11, 2000,)