COMPUTER-RELATED OFFENCES

A presentation at the Octopus Interface 2004 - Conference on the Challenge of Cybercrime, 15-17 September 2004, Council of Europe, Strasbourg, France.

Stein Schjolberg
Chief judge
Moss tingrett
Norway
E-mail: steins@mosstingrett.no
www.cybercrimelaw.net
www.globalcourts.com

I. THE BACKGROUND

The first initiative on computer crime in Europe was the Council of Europe Conference on Criminological Aspects of Economic Crime in Strasbourg in 1976.[1] Categories of computer crime were introduced, including fraud.

The first comprehensive initiative on computer crime in the United States was a staff study by the U.S. Senate Government Operations Committee in February 1977. This staff study addressed several problems associated with computer programs, and recommended that legislation should be considered that would prohibit unauthorized use of computers. The Chairman of this committee was Senator Abe Ribicoff.[2]

Senator Ribicoff introduced the Ribikoff Bill later in 1977. This Bill was the first proposal for Federal computer crime legislation in the U.S. that would

[1] 12th Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime, Strasbourg, 15-18 November 1976, page 225-229.
[2] Staff Study of Computer Security in Federal Programs; Committee on Governmental Operations, the 95th Congress 1 Session, United States Senate, February 1977

specifically prohibit misuse of computers. The Bill S. 1766 (95th Congress) was cited the "Federal Computer Systems Protection Act of 1977".[3] Senator Ribikoff stated in his presentation, still valid today:

"Our committee investigation revealed that the Government has been hampered in its ability to prosecute computer crime. The reason is that our laws, primarily as embodied in title 18, have not kept current with the rapidly growing and changing computer technology. Consequently, while prosecutors could, and often did, win convictions in crime by computer cases, they were forced to base their charges on laws that were written for purposes other than computer crime. Prosecutors are forced to "shoe horn" their cases into already existing laws, when it is more appropriate for them to have a statute relating directly to computer abuses."[4]

The Bill was not adopted, but this pioneer proposal became the model legislation in state computer crime legislation in the United States and created awareness all around the world.

Interpol was the first international organization addressing computer crime and penal legislation[5] in 1979. In conjunction with the Interpol Conference in 1981[6], a survey of Interpol member countries on computer crime and penal legislation identified several problems in the application of existing penal legislation.

The OECD in Paris appointed in 1983 an expert committee to discuss computer-related crime and the need for changes in the Penal Codes. This committee made a proposal that could constitute as a common denominator between the different

[3] Congressional Records, 95th Congress, Vol. 123, No. 111, June 27, 1977
[4] Congressional Records, 95th Congress, Vol. 123, No. 111
[5] The Third Interpol Symposium on International Fraud, Saint-Cloud, Paris, France, December 11-13, 1979.
[6] The First Interpol Training Seminar for Investigators of Computer Crime, Saint-Cloud, Paris, France, December 7-11, 1981. The keynote speaker at the conference was Donn B. Parker, SRI International, USA, and the "founder" of the combat against computer crime.

approaches taken by the member countries, including fraud and forgery as follows:[7]

" a) the input, alteration, erasure and/or suppression of computer data and/or computer programs made wilfully with the intent to commit an illegal transfer of funds or of another thing of value;
b) the input, alteration, erasure and/or suppression of computer data and/or computer programs made wilfully with the intent to commit a forgery;

The Council of Europe appointed in 1985 another expert committee in order to discuss the legal issues of computer–related crime. A summary of the guidelines for national legislatures with liability for intentional acts only, was presented in the Recommendation of 1989 and included computer fraud and forgery as follows:[8]

a) Computer fraud.
The input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, that influences the result of data processing thereby causing economic or possessory loss of property of another person with the intent of procuring an unlawful gain for himself or for another person (alternative draft: with the intent to unlawfully deprive that person of his property).
b) Computer forgery.
The input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, in a manner or under such conditions, as prescribed by national law, that it would constitute the offence of forgery if it had been committed with respect to a traditional object of such an offence.

The United Nations adopted a resolution[9] on computer crime legislation at the 8th U.N. Congress on the Prevention of Crime and the Treatment of Offenders in Havana, Cuba, in 1990. The United Nations Manual on the Prevention and Control of Computer-related Crime was published in 1994. A new resolution was adopted by the General Assembly in 2000 on combating the criminal

[7] Computer-related criminality: Analysis of Legal Politics in the OECD Area (1986)
[8] Computer-related crime: Recommendation No. R. (89) 9, see http://cm.coe.int/ta/rec/1989/89r9.htm
[9] The resolution was adopted by the General Assembly on December 14, 1990

misuse of information technologies[10]. In this resolution it was noted the value of certain measures to combat the criminal misuse of information technologies, including:

"States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies."

The last part of this historic presentation is the Wurzburg conferences organized by the University of Wurzburg in 1992.[11] These conferences introduced 29 national reports, and recommendations for the development of computer crime legislations.

Most countries in Europe adopted new penal laws according to the recommendations of the 1980's. Similar development occurred in the USA, Canada and Mexico. In Asia Japan, Singapore, Korea and Malaysia were the leading countries. In Australia, the Commonwealth added computer crime laws to the Crimes Act in 1989.

II. THE CYBERSPACE AGE - INTERNATIONAL LEGAL INSTRUMENTS

The G 8 countries established in 1997 the Subgroup of High-Tech Crime. At a meeting in Washington D.C. in 1997[12], the G8 countries adopted Ten Principles

[10] The resolution was adopted by the General Assembly on December 4, 2000 (A/res/55/63)
[11] See Ulrich Sieber (ed): Information Technology Crime – National Legislations and International Initiatives, Carl Heymanns Verlag KG (1994).
[12] The Washington Communique of December 10, 1997

in the combat against computer crime. The goal was to ensure that no criminal receives "safe havens" anywhere in the world.

At the last Meeting of G-8 Justice and Home Affairs Ministers in Washington D.C., on May 10-11, 2004,[13] a joint communiqué was issued, including as follows:

"**Continuing to Strengthen Domestic Laws.** To truly build global capacities to combat terrorist and criminal uses of the Internet, all countries must continue to improve laws that criminalize misuses of computer networks and that allow for faster cooperation on Internet-related investigations. With the Council of Europe's Convention on Cybercrime coming into force on July 1, 2004, we should take steps to encourage the adoption of the legal standards it contains on a broad basis"

Stanford University in California, organized in December 1999 a Conference on International Cooperation to Combat Cyber Crime and Terrorism.

Based on the experience at the conference, Stanford University introduced in 2000 a Proposal for an International Convention on Cyber Crime and Terrorism.[14]

In the European Union, the Commission of the European Communities presented on April 19, 2002 a proposal for a Council Framework Decision on attacks against information systems.[15]

The Council of Europe Convention on Cybercrime was opened for signatures at a Conference in Budapest, Hungary, on November 23, 2001.[16]The Convention is

[13] See http://www.usdoj.gov/ag/events/g82004/index.html
[14] See http://cisac.stanford.edu
[15] See http://europa.eu.int/information_society/topics/telecoms/internet/crime/index_en.htm

a historic milestone in the combat against cyber crime, and entered into force on July 1, 2004.

The Ministers of Justice or Ministers or Attorneys General of the Americas in the Organization of American States (OAS) recommended in Peru in 1999 the establishment of a group of governmental experts on cybercrime. Consideration of recommendations was discussed at a meeting in Washington D.C., June 23-24, 2003. The Fifth Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas in Washington D.C. on April 28-30, 2004,[17] approved conclusions and Recommendations to the General Assembly of the OAS, including as follows:

"That Member States evaluate the advisability of implementing the principles of the Council of Europe Convention on Cybercrime (2001), and consider the possibility of acceding to that convention."

At the meeting in Mexico in October 2002 APEC[18] leaders collectively committed to:

"Endeavour to enact a comprehensive set of laws relating to cybersecurity and cybercrime that are consistent with the provisions of international legal instruments, including United Nations General Assembly Resolution 55/63 (2000) and Convention on Cybercrime (2001), by October 2003."

At an APEC seminar in Bangkok, Thailand, on July 21-25, 2003, it was agreed, including that:

---

[16] See http://conventions.coe.int/treaty/EN/projets/FinalCybercrime.htm
[17] See http://www.oas.org/juridico/english/cyber.html
[18] See http://www.apectelwg.org

"International instruments, in particular the Council of Europe Cybercrime Convention (2001), provide valuable models for improving domestic laws."

Based on the Council of Europe Convention on Cybercrime, we may reach our goal, as expressed by President Jacques Chirac of France at the G-8 Meeting in 2000: a rule of law at an international level, a universal legal framework equal to the worldwide reach of the Internet.[19]

Outside Europe, the U.S. Department of Justice has been very active in the establishment of regional solutions for OAS and APEC on cybercrime laws in accordance with the convention.

III. LAW COMES TO CYBERSPACE

Cyberspace has developed since the 1990's, and the impact on societies has been so fast and enormous, that code of ethics, common sense of justice and penal laws has not kept pace.

In order to establish ethical behaviours in Cyberspace, penal laws must be enacted with as much clarity and specificity as possible, and not rely on vague interpretations in the existing legislation. With cybercrime laws, perpetrators will be convicted for their explicit acts and not by existing provisions stretched in the interpretation, or by provisions enacted for other purposes covering only incidental or peripheral conduct.

[19] President Jacques Chirac, at the G-8 Meeting in France 2000.

Any regulation of unlawful conduct involving the use of Internet should be analysed through a policy framework that ensures that online conduct is treated in a manner consistent with the way offline conduct is treated, in a technology-neutral manner that accounts for other important societal interests such as privacy and protection of civil liberties.[20]

It will also ease the evidentiary burden for law enforcement and prosecutors, and the courts will be able to participate in the process of establishing ethical standards more significantly through their ruling and sentencing.

The nature of cybercrime and the legal issues are global. Through international organizations, such as the Council of Europe, efforts has been taken to ensure the harmonization of provision in the individual countries. Ensuring that the dual criminality requirement is fulfilled may provide for an efficient global prosecution of cybercrimes. Such approach is especially vital in the investigation and prosecution of attacks against the infrastructure of computer systems and networks.

Countries must be able to prosecute cybercrimes committed by national individuals or any person domiciled in that country, whenever the acts are committed abroad. And each country should also be able to prosecute a foreigner present in the country, whenever it does not extradite the person after a request for extradition for cybercrimes committed abroad.

[20] The Electronic Frontier: The Challenge of Unlawful Conduct involving the use of the Internet – A Report of the President's Working Group on Unlawful Conduct on the Internet. (US March 2000)

In order to make a proposal for the ratification of the Council of Europe Convention on Cybercrime, many member countries has established Cybercrime Expert Committees.

After signing the Council of Europe Convention on Cybercrime in Budapest in November 2001, the Norwegian Government appointed in 2002 a Cybercrime Committee (Datakrimutvalget). It was decided that our commission was split in two reports. The first report should consist of a proposal for the necessary amendments in the penal code and the criminal procedural law only for the ratification of the Convention. The second report should cover a broader approach with an overview of all possible amendments in the penal and procedural provisions needed in the information and communication technology of computer systems and networks.

Our strategy was therefore using declarations according to art. 40, and reservations according to art. 42, whenever it was possible. The report was presented to the Minister of Justice on November 4th 2003.[21]

The answers in Norway and many countries that adopted provisions in the Penal Code according to the Recommendations of the 1980's are: Yes, we are covered, with the exception of Article 6: Misuse of devises.

IV. SUBSTANTIVE CRIMINAL LAW-COMPUTER-RELATED OFFENCES

[21] http://www.odin.dep.no/jd/norsk/publ/utredninger/NOU/012001-020027/index-dok000-b-n-a.html

The term computer-related crime was historically used in describing all categories of crimes involving computers, but it is used in the convention in a narrow sense, covering only computer forgery and computer fraud.

Forgery and fraud are traditional criminal offences where computer systems are used as tools in the cyberspace dimension of such activities.

1. Computer-related forgery

Article 7 – Computer-related forgery:

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

The provisions of forgery requires in most countries visual readability of statements or declarations embodied in a document and therefore do not cover computer data.

Computer data that is either of significance as evidence of any right, obligation or exemption therefrom or appears to be designed to serve as evidence, must be protected in the similar manner as paper-based documents. Manipulations of such data may have the same serious consequences and should be a crime in the same manner as traditional forgery of documents.

It is the security and reliability of computer data that may have consequences on legal transactions and are legally relevant that must be protected.

Computer-related forgery involves unauthorized creating or altering stored data so that they acquire a different evidentiary value in the course of legal transactions, which relies on the authenticity of information contained in the data, subject to a deception.[22]

In article 7 "input" of correct or incorrect data corresponds to the making of a false document. "Alterations" (modifications, variations, partial changes), and "deletions"(removal of data from a data medium), and "suppression"(holding back, concealment of data) correspond in general to the falsification of a genuine document.[23]

Some countries have statutes on forgery including visual readability with the aid of technical means, which may cover computer-related forgery. Other countries has included "electronically", "or on which information is recorded or stored by electronic or other means" in the definition of documents. But countries with traditional statutes on forgery including: "any object that in writing or otherwise contains a statement" may be a too vaguely worded rule.

Categories of Internet forgery may include: bogus Websites that falsely present themselves as the sites of established companies for fraudulent purposes, or assumption of false identity in e-mail messages for fraudulent purposes, or the posting of false information on Internet bulletin boards to manipulate stock market prices.

Sale or distribution of false identification documents through computer files or

[22] Explanatory Report to the Convention on Cybercrime no. 81
[23] Explanatory Report to the Convention on Cybercrime no 83

computer templates are illegal. It is also illegal placing a template for making false identifications on a Website or other online location available to others.
A fake identification template is a computer file; usually in Adobe PhotoShop format, which can be modified, printed, and laminated, with the intent of resembling a real license, e.g. driver's license.
Another scam is the electronic price tag alteration, where online retailers are the victims.
The offence must be committed intentionally and without right. But Article 7 allows countries also to require a specific intent to defraud or similar dishonest intent, before criminal liability attaches.[24]

2. Computer-related fraud

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another by:
a. any input, alteration, deletion or suppression of computer data,
b. any interference with the functioning of a computer system,
with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another.

[24] Explanatory Report to the Convention on Cybercrime, no. 85

Computer fraud is conduct which involves the manipulation of a computer, by whatever method, in order dishonestly to obtain money, property or some other advantage of value or to cause loss.[25] In most countries the traditional provisions of fraud requires a deception of a human being. It is not possible to deceive a computer within the meaning of deception in this required sense, and consequently new provisions covering computer-related fraud have been enacted.

The traditional elements of committing fraud are still valid on computer fraud in Cyberspace. They are: (1) by the use of incorrect or incomplete information (2) by altering data or programs, or otherwise unlawfully influences the result of computer operations (3) that causes a loss of property or a risk of loss to anyone, (4) with the intent of procuring an unlawful economic gain for himself or for another person.

Article 8 includes any input, alteration, deletion, suppression of computer data, or any interference with the functioning of a computer system. The aim of the Article is to "criminalize any undue manipulation in the course of data processing with the intention to effect an illegal transfer of property."[26] The act must cause a loss of property, and in addition to the traditional property e.g. money, it must be understood as anything of economic value.

Internet frauds have become a global issue due to the rapid development of the Internet. In countries that have updated the fraud provisions based on the

[25] The Law Commission, Report No. 186, Criminal Law-Computer Misuse, 1989, England
[26] Explanatory Report to the Convention on Cybercrime, no 86

recommendations of the 1980's, existing laws may generally be adequate with regard to the article 8. But perpetrators often design new forms of fraud to exploit opportunities offered by the Internet.

Internet fraud includes several categories of schemes. It may be false or misleading offerings involving all kinds of property, promises, unfounded financial projections. It may be credit card fraud, mail fraud or bank fraud.

A typical fraud on the Internet is stock fraud or online securities fraud. Companies and individuals are using the Internet to artificially inflate the market value of stocks by creating demand for less traded low priced stocks. Unsolicited e-mails, electronic newsletters, message boards and Web sites are used as tools to commit such frauds.

Another typical fraud in Cyberspace is price tag frauds or fraud involving online retail sales.

Electronic price tag alterations on Web sites is a growing concern in e-commerce. After choosing a product and receiving pricing information on a commercial Web page a perpetrator may be able to alter price information.

But the most common of all frauds in Cyberspace is online auction fraud.

In a report made by the Internet Fraud Complaint Center (IFCC) estimates in 2001 that online auction frauds entails 64% of all Internet frauds that is reported in the U.S., with an average loss per complaint amounting to USD 776.[27]

[27] See Internet Fraud Complaint Center (IFCC), Internet Auction Fraud, May 2001, http://www.1.ifccfbi.gov

According to this report the most popular items on Internet auctions are: "beanies" (small stuffed animals), cameras/camcorders, desktop computers, jewelry, laptop computers, and video consoles/games/tapes. But online auction frauds are global scams and victims are from around the world. In the most typical frauds perpetrators are often using numerous fictitious names and e-mail addresses, receiving payment but never intended to deliver the purchased goods. "Shell bidding" is a practice of false bidding by the seller and/or conspirators designed to drive up the price of an item and force unknowing bidders to increase their bids to acquire the item.[28]

Committing computer-related fraud requires the general intent element covering art 8 a and b, and in addition the specific fraudulent or dishonest intent to gain an economic or other benefit for himself or another.

V. CONCLUSION

The articles on computer-related offences poses few challenges in the ratification process.

Countries that have updated the forgery and fraud provisions based on the recommendations of the 1980's may find the existing laws adequate with regard to the articles 7 and 8.

But criminal laws on forgery that requires visual readability of statements or declarations embodied in a document may not cover computer data. The

[28] See Paula Selis, Anita Ramasastry and Charles S. Wright: Toward a fraud-free marketplace – best practices for the online auction industry.

definition of documents may also need to be updated.