Current Topics in Law and Legislation

The following section provides an overview of the main national and international respectively EU-level legal issues in the area of CIIP. The development of effective regulation, law, and criminal justice mechanisms are essential in deterring virtual abuse and other offences against information infrastructure. Moreover, a strict regulation may create trust in the new ICT and encourage the private sector and individuals to make better use of e-Commerce or e-Government services.

The following is an overview of important common issues currently discussed in the context of legislation procedures in the countries covered in the handbook:[48]

- Data protection and security in electronic communications (including data transmission, safe data storage, etc.);
- IT security and information security requirements;
- Fraudulent use of computer and computer systems, damage to or forgery of data, and similar offences;
- Protection of personal data and privacy;
- Identification and digital signatures;
- Responsibilities in e-Commerce and e-Business;
- International harmonization of cybercrime law;
- Minimum levels of information security for (e-)governments, service providers, and operators, including the implementation of security standards such as BS7799, the code of practice for information security management ISO/IEC 17799, the Common Criteria for Information Technology Security Evaluation ISO/IEC 15408, and others;
- Public key infrastructure and its regulation.

48 Finnish Communications Regulatory Authority. *Information Security Review Related to the National Information Security Strategy* (24 May 2002). http://www.ficora.fi/englanti/document/review.pdf; includes information on national approaches from experts involved.

International Level

Due to the inherently transnational character of CI/CII, there is a need to harmonize national legal provisions and to enhance judicial and police co-operation. However, so far, the international legal framework has remained rather confused and is actually an obstacle to joint action by the actors involved.

At the European level, the *Council of Europe Convention on Cybercrime* and the proposed *European Framework Decision on Attacks Against Information Systems* are currently among the most important pillars of transnational CIIP legislation efforts.

Council of Europe Cybercrime Convention

International cooperation is crucial when it comes to tackling cybercrime. The most important legislative instrument in this area is the *Council of Europe Cybercrime Convention*[49], which was signed on 23 November 2001 by twenty-six members and four non-members of the Council. The Convention is the first international treaty on crimes committed via the Internet and other computer networks. Its main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation.[50] An additional protocol to the Convention outlaws racist and xenophobic acts committed through computer systems. The criminal offences concerned are:

- Crimes against the confidentiality, integrity, and availability of computer data or systems, such as spreading of viruses;
- Computer-related offences such as virtual fraud and forgery;
- Content-related offences, such as child pornography;
- Offences related to infringements of intellectual property and related rights;

Another objective of the convention is to facilitate the conduct of criminal investigations in cyberspace.[51]

49 http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm.
50 http://conventions.coe.int/Treaty/en/Summaries/Html/185.htm.
51 http://press.coe.int/cp/2001/893a(2001).htm.

European Framework Decision on Attacks Against Information Systems

An important step is the *Framework Decision on Attacks against Information Systems*, as proposed by the *European Commission* in April 2002.[52] The Framework seeks to address cybercrime in a harmonized manner throughout Europe, including prosecuting attacks against critical civil infrastructures such as power plants, water supply systems, airports, and hospitals. It also plans to ensure that European law enforcement authorities can take action against offences involving illegal access, hacking, or interference with information systems, such as denial of service attacks, web-site defacements, and viruses.

Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries

Computer Security Incident Response Teams (CSIRTs) operate in an environment where the legal codes of the different member states diverge in dealing with computer crime and misuse. Moreover, the law enforcement authorities of the EU member states often have varying approaches to similar problems. Therefore, the *Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries*[53] was designed to help Europe's CSIRT to meet the challenge of dealing with incidents. The handbook was funded by the EC and commissioned to RAND Europe, who led the project.

The *Handbook of Legislative Procedures* is useful for organizations involved in the incident-handling phase (e.g., CSIRTs and CERTs) and for law enforcement agencies engaged in incident response and investigation. Although the handbook focuses on the 15 EU member states, it is also of interest to CSIRTs in other countries.

The *Handbook of Legislative Procedures* has two sections: The first covers incident descriptions, international legal and forensic principles, and incident surveys. Particular attention is paid to the examination of the content of the *Council of Europe's Cybercrime Convention* and the proposed *European Framework Decision on Attacks Against Information Systems*. The second

52 Commission of the European Communities. *Proposal for a Council Framework Decision on Attacks Against Information Systems.* COM (2002) 173 final. http://europa.eu.int/eur-lex/en/com/pdf/2002/com2002_0173en01.pdf.

53 http://www.iaac.org.uk/csirt.htm.

section of the handbook contains an analysis for each EU member state and its legislation in the area of computer crime.[54]

Cyber Tools On-Line Search for Evidence (CTOSE)

The *EU Cyber Tools On-Line Search for Evidence* (CTOSE)[55] project, a research project funded by the *European Commission's Information Society Technologies* (IST) program, has developed forensic standards for prosecuting cybercrime. The standards are based on a methodology that identifies, secures, integrates, and presents electronic evidence. This methodology should enable system administrators, information technology security staff and computer incident investigators, police and law-enforcement agencies, etc., to follow consistent and standardized procedures when investigating computer incidents. Furthermore, the methodology ensures that all electronic evidence is gathered and stored in a way that meets legal standards. Backers of the methodology hope it will be adopted as a best-practice standard throughout Europe.[56]

National Level

Although many developed countries have been concerned with the protection and security of information (infrastructures) and related legislation for some years, they have only begun to review and adapt their CIIP legislation after 11 September 2001. Because national laws are developed autonomously, some countries have preferred to amend their penal or criminal code, whereas others have passed specific laws on cybercrime.

National Examples

This section lists some interesting examples of CIIP legislation. This includes a wide variety of acts defining the responsibilities of the government authorities in case of emergencies, as well as legislation dealing with issues such as technical IT security, data protection, damage to data, fraudulent use of a computer, the handling of electronic signatures, etc. Several countries have begun reviewing their legislation since 11 September 2001.

54 RAND Europe. *Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries* (study for the European Commission Information Society Directorate-General, 2002). http://www.iaac.org.uk/CSIRT%20Handbook-v24.pdf.

55 http://www.ctose.org.

56 http://www.ctose.org/info/index.html.

Legal Issues in Australia

The *Australian Security Intelligence Agency* (ASIO) has the power to covertly enter and search the premises of those it suspects of espionage or terrorism. The *ASIO Act* (1979) was subsequently amended *(ASIO Amendment Act)*[57] in 1999, to give the organization the same covert access to targets' computer systems.

The Australian Government has introduced new computer crime legislation, the *Cybercrime Act* (2001),[58] to implement the rulings on computer offences proposed in the recently released *Model Criminal Code Report*.[59] This is an important step toward achieving national consistency in this area and remedying the deficiencies in existing laws. Mirror legislation has already been implemented in New South Wales, and other states are also expected to follow suit. The proposed legislation on computer offences is designed to protect the security, integrity, and reliability of computer data and electronic communications. It is hoped that the penalties will provide a strong deterrent to those who engage in cybercrime such as hacking, computer virus propagation, and denial of service attacks. Serious offences, such as stalking and fraud, are also covered.[60]

Since the introduction of the *Cybercrime Act* (2001),[61] the ASIO has enjoyed considerably more leeway and may now conduct CIIP investigations. Under new counter-terrorism legislation introduced in 2003, the ASIO can detain and question suspects without charge for up to seven days. Previously, the ASIO had not been allowed to interrogate suspects, and relied on the *Australian Federal Police* (AFP) to carry out police actions on its behalf or based on the intelligence that the ASIO had covertly generated.

The introduction of the *Cybercrime Act* (2001) prompted the AFP to join forces with state and territory police to create a national organization against cybercrime. The line dividing cybercrime and cyberterrorism is blurred, because many of the tools and techniques are common to both activities.

Further Acts:

- Crimes Act 1901 Part VIA: This act deals with attacks against computers in Australia, and with all computer attacks using the Australian telecommunications system;

57 http://www.aph.gov.au/library/pubs/bd/1998-99/99bd172.htm#Passage.

58 http://www.aph.gov.au/library/pubs/bd/2001-02/02bd048.htm.

59 http://www.aic.gov.au/links/mcc.html.

60 Interview with a representative of the National Office for the Information Economy (NOIE), July 2002.

61 http://www.aph.gov.au/library/pubs/bd/2001-02/02bd048.htm.

- Telecommunications (Interception) Act 1979: This act prohibits the interception of telecommunications (including data transmissions) within Australia, except under warrant. There are also provisions in the *Telecommunications Act of 1997* that require carriers or carriage service providers to enter into an agreement with the government about planning for network survivability or operational requirements in time of crisis, and which stipulate that rules and licenses for carriers or service providers may require compliance with a disaster plan;
- Radiocommunications Act 1992: This act covers offences relating to radio emission, including interference likely to prejudice the safe operation of aircraft or vessels, interference with certain radio communications, and interference likely to cause danger, loss, or damage.

Legal Issues in Italy[62]

Italy has specific laws and ministerial decrees devoted to CIP and CIIP. In the early 1990s, a new law related to computer crimes was introduced (Law 547 of 23 December 1993), giving more power to investigators in the evidence-collection phase, and also allowing computer and telecommunication interceptions. Italy was one of the first European countries to adopt such legislation, mainly due to new crime figures concerning computer frauds, forgery, data damaging, computer misuse, unauthorized interceptions of computer communications, and sabotage. The great attention given to such crimes is highlighted by the fact that computer intrusions are treated as a domestic property violations.

An innovative concept of *High-Tech Crime*, which already enjoyed currency in the Italian penal legislation for different type of offences, was introduced with Law 547. According to article 420 of the *Italian Penal Code* (attempt to damage public utilities systems), actual damage or destruction to the systems are not required for such activities to constitute an offense; the mere intention suffices. Such cases will be prosecuted, even if the attempt has not been successful.

Other relevant laws include:

- Law 547, enacted on 23 December 1993, a comprehensive and integrated law against ICT crimes;

62 Information based on Roberto Setola, Secretary of the Working Group on Critical Infrastructure Protection coordinated by the Cabinet Office of the Italian Government.

- Legislative Decree 518, enacted on 29 December 1992 and modified by Law 248 (18 August 2000), a legislative decree against illicit ICT piracy;
- Law 675, enacted on 31 December 1996, a law governing personal data protection, integrated by subsequent legislation (DPR 318/1999, Law 325/2000, Legislative Decree 467/2001, and Legislative Decree 196/2003);
- Legislative Decree 374/2001, changed into Law 438/2001, a law devoted to better law enforcement instruments and the repression of terrorism.

Note that Law 374/2001, transformed into Law 438/2001 after 11 September 2001, has updated the Penal Code, so that now, crimes committed in Italy are liable to prosecution, even if they are directed against a foreign state or against a multilateral institution.

Legal Issues in New Zealand

The *Crimes Amendment Act* came into force in October 2003. It includes four new offences relating to the misuse of computers and computer systems. These offences are:

- Accessing a computer system for a dishonest purpose (section 249);
- Damaging or interfering with a computer system (section 250);
- Making, selling, or distributing or possessing software for committing a crime (section 251);
- Accessing a computer system without authorization (section 252).

The expressions "access" and "computer system" are defined in section 248.

The first two offences carry a range of penalties depending on the seriousness of the offence, with a maximum of 7 and 10 years imprisonment respectively, while the remainder carries a maximum penalty of 2 years imprisonment.

The section 249 offence involves accessing a computer system directly or indirectly, either to obtain a benefit for oneself or to cause loss to another person, or with intent to do so. The essential element of the offence in either case is dishonesty, or deception (which is separately defined in section 240(2)).

The section 250 offence involves intentional or reckless destruction, damage, or alteration of a computer system. At its most serious, if this is done by a person who knows or ought to know that danger to life is likely to result, the section provides a maximum penalty of 10 years imprisonment. Where a person damages, deletes, modifies or otherwise interferes with or impairs any data or software without authorization, or causes a computer

system to either fail or deny service to any authorized users, the maximum penalty is 7 years imprisonment.

The key element of the section 251 "sale, supply, or distribution" offence is that the person must either know that a crime is to be committed, or must promote the software in question as being useful for the commission of a crime, knowing that or being reckless as to whether it will be used for such a purpose. In the case of the "possession" offence, the key element is intention to commit a crime.

The more significant in practice of these two offences is likely to be section 252, which in effect makes computer "hacking" a criminal offence. The offence is simple unauthorized access, whether direct or indirect, to a computer system, knowing that or being reckless as to whether one is unauthorized to access that computer system.

Sections 253 and 254 contain qualified exemptions in respect of the section 252 offence for the *New Zealand Security Intelligence Service* and the *Government Communications Security Bureau* respectively, where those organizations are acting under the authority of (in the case of the NZSIS) an interception warrant or (in the case of the GCSB) a computer access authorization issued under section 19 of the GCSB Act 2003.

Legal Issues in Norway

The §151b of the Penal Code states that whosoever causes comprehensive disturbances to the public administration or other parts of society by disrupting the collection of information, or by destroying or damaging power supply plants, broadcasting facilities, telecommunications services, or other kinds of communication, will be punished by a maximum of 10 years imprisonment. Unlawful negligence as mentioned in the first instance will be punished by incarceration for a maximum of 1 year. Accessories will be punished in the same manner. This law came into effect on 12 June 1987.[63]

In Norway, the laws generally tend to place responsibility firmly with the operator in cases of accidents such as rail crashes or fires. However, during the last years, systemic errors and bad leadership have become apparent as the underlying causes of many accidents.[64]

63 Information provided by a Norwegian expert of the Directorate for Civil Defense and Emergency Planning (DSB), March 2002.

64 http://www.ocb.se/dokument/filer/5b_gjengsto_henriksen_abstract.pdf.

Legal Issues in Switzerland

A number of articles in the Swiss Penal Code are of relevance in the context of CIIP.

- Article 143 (unauthorized procurement of data);
- Article 143bis (unauthorized access to a computing system): This article states that any person that, by means of a data transmission device, gains unauthorized access to a computing system belonging to others, and specially protected against access by the intruder, shall be punished by imprisonment or a fine if a complaint is made;[65]
- Article 144 (damage to property): The article states that any person that damages, destroys, or renders unusable any property belonging to others, shall be punished by imprisonment or a fine if a complaint is made;[66]
- Article 144bis (damage to data): The article states that any person that alters, deletes, erases, or renders unusable data stored or transferred by electronic or similar means without authorization, shall be punished by imprisonment or a fine if a complaint is made;[67]
- Article 147 (fraudulent use of a computer): The article states that any person that, with the intention of unlawfully obtaining financial rewards for himself or another, interferes with an electronic procedure through the unauthorized use of data, shall be punished by community service of up to five years or imprisonment;[68]

Although the *Swiss Penal Code* is up to date, only a few cases have been prosecuted so far. Switzerland's laws against virus creation and the use of malicious software in general are widely applicable. However, the legal structure in Switzerland makes prosecution difficult, due to the complexities of different laws (comprised of laws on both the federal and cantonal level) and law enforcement procedures.

In November 2001, the Federal Council accepted the "*Convention on Cybercrime of the Council of Europe*".[69] It should be noted that the Swiss

65 Based on the official English translation of the Swiss Penal Code.
66 Based on the official English translation of the Swiss Penal Code.
67 Based on the official English translation of the Swiss Penal Code.
68 Based on the official English translation of the Swiss Penal Code.
69 ISPS News (Infosociety.ch), press release: *Gemeinsam die Cyber-Kriminalität bekämpfen. Bundesrat genehmigt Konvention des Europarats*. http://www.isps.ch.

Penal Code is already in agreement with the corresponding international articles on infringements of copyright, computer-related fraud, child pornography, and offences related to unauthorized intrusion into protected computer systems.

Legal Issues in the US

In the US, legislative awareness of computer crimes grew dramatically in the early 1980s, as computers became increasingly important for the conduct of business and politics. The *Computer Fraud and Abuse Act* (CFAA) of 1986 was the conclusion of several years of research and discussion among legislators.[70] It established two new felony offenses consisting of unauthorized access to "federal interest" computers[71] and unauthorized trafficking in computer passwords. Violations of the CFAA include intrusions into government, financial, most medical, and "federal interest" computers.

The *Computer Abuse Amendments Act* of 1994 expanded the 1986 CFAA to address the transmission of viruses and other harmful code.[72] The measures provided by this act were further tightened on 26 October 2001 by the *USA PATRIOT* anti-terrorism legislation.[73] Violations of the CFAA are investigated by the *National Computer Crimes Squad* at the FBI and supported by its *Computer Analysis and Response Team* (CART), a specialized unit for computer forensics.[74]

Much of the federal legislation concerning CIP/CIIP was written before the emergence of "cyberthreats". Thus, it is questionable whether a timely and efficient response would be possible under the existing legal frameworks at both federal and state/local levels.[75]

70 http://www4.law.cornell.edu/uscode/18/1001.html.

71 Federal interest computers are defined as two or more computers involved in a criminal offense, if they are located in different states.

72 See also http://www.digitalcentury.com/encyclo/update/comfraud.html Jones Telecommunications and Multimedia Encyclopedia.

73 USA PATRIOT stands for: *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*. For full text version see http://www.cdt.org/security/usapatriot/011026usa-patriot.pdf. Privacy and civil liberty advocacy groups have expressed concern over a number of legislative developments.

74 http://www.fbi.gov/hq/lab/org/cart.htm. Of further importance is also the recent enactment of the Gramm-Leach-Bliley (GLB) Act and the regulations that implement GLB, which address privacy concerns by setting forth a range of requirements to protect customer information. For text of GLB, see http://www.ftc.gov/privacy/glbact.

75 President's Commission on Critical Infrastructure Protection, Critical Foundations, p. 81.

While the overall act established the *Department of Homeland Security* (DHS), Title II of the *Homeland Security Act* (of 2002) specifically addresses information analysis and infrastructure protection. It created the *IAIP Directorate*, transferred the various agencies (like CIAO, NIPC, and others mentioned above) into the DHS, and established the categories of information to which the secretary of homeland defense has access. In order to adequately protect the nation, the secretary has access to certain intelligence analysis, infrastructure vulnerabilities, and any "raw" data that the president discloses to the secretary.

CIIP is an important issue in the US, primarily because many of critical sectors are regulated by the government, but controlled by private entities. As part of the regulation, the private entities must regularly file reports and disclose sensitive information to the government. This could place such information in jeopardy, since under the *Freedom of Information Act* (FOIA), the public can request such information from the government. However, as part of the Homeland Security Act of 2002, a *FOIA exemption* was created. Any information regarding critical infrastructures (including security systems, warnings, or interdependency studies) is exempt from disclosure.

The "*Terrorism Risk Insurance Act of 2002*" is a new law that creates a federal program for public and private compensation for insured losses resulting from acts of terrorism. All commercial insurance providers must offer terrorism risk insurance, and the federal government agrees to underwrite some of the losses in the event that a terrorist event takes place. Under this law, an act of terrorism includes any act of violence against infrastructure.[76] This could include catastrophic network assaults as well as physical attack.

After the attacks of 11 September 2001, the *Federal Energy Regulatory Commission* (FERC) removed certain information from its website and its public reading room. This included detailed maps and other information about electric power facilities and natural gas pipelines. Although exempt from FOIA procedures, this information had traditionally been open and available to anyone who requested it. In February, 2003, FERC ruled that individuals wanting access to this information would have to apply for it. The application requirements include identification information, and take the need/purpose of the information into account. Access is granted on a case-by-case basis, and only to individual applicants.

76 Terrorism Risk Insurance Act of 2002, Pub. L. No. 107–297, 116 Stat. 2322 (2002).

Center for Security Studies, ETH Zurich
Volume 2, Zürich 2004.

The International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries

Myriam Dunn and Isabelle Wigert

edited by
Andreas Wenger and Jan Metzger