Prof. Dr. Christian Schwarzenegger

Computer crimes in Cyberspace
A comparative analysis of criminal law in Germany, Switzerland and Northern Europe

This article aims to give an overview of the current state of criminal legislation, the case law and the legislative initiatives in the field of computer crimes, particularly in view of the ratification of the CoE «Cybercrime Convention». Special attention is given to the criminal responsibility for the distribution and production of computer-viruses, for illegal access to computer systems (hacking), and for data-spying in Germany, Switzerland and Northern Europe.

Outline of the report

[Rz 1] The report aims to give an overview of the current state of criminal legislation, the case law of the countries under examination and the legislative initiatives in the field of computer crimes, particularly in view of the ratification of the CoE "Cybercrime Convention" (see Schwarzenegger 2002, 305 et seq.). Jurisdictional issues play a prominent role in the prosecution of borderless cybercrimes; however, they are not dealt with in this report. An overview on penal jurisdiction in Germany, Switzerland and Austria is given in Schwarzenegger (2000, 109 et seq. with further references; see also the recent decision by the German Federal High Court, 12 December 2000 - 1 StR 184/00, Neue Juristische Wochenschrift 2001, 624 et seq. = sic! 2001, 240 et seq.)

[Rz 2] Priority will be put on the analysis of the German and Swiss penal law. Second, some additional material on Scandinavian countries will be included.

A. Germany

[Rz 3] Several provisions of the Penal Code can be applied to attacks on computer systems: Computer fraud (§ 263a Penal Code), falsification of data with proof-relevance (§ 269 Penal Code), alteration of data (§ 303a Penal Code), computer sabotage (§ 303b Penal Code), data spying (§ 202a Penal Code) and others.

Table 1: Computer crimes known to the police (1995-1999, entire country)

year	1995	1996	1997	1998	1999
Computer fraud (§ 263a)	3575	3588	6506	6465	4474
alteration of data and computer sabotage (§§ 303a, 303b)	192	228	187	326	302
data spying (§ 202a)	110	933	213	267	210

[Rz 4] According to the Criminal Statistics of the Police the incidence rate of computer crimes is going up and down (see Table 1). It has to be mentioned that these statistics do not list Internet-related offences separately.

[Rz 5] These figures concern crimes known to the police. The following table (see Table 2) shows the number of convictions for computer crimes, which have been pronounced between 1995 and 1999 (again, the statistics do not allow for a separate analysis of Internet-related offences, the numbers include only sentences from the old territory of the German Federal Republic plus Berlin East&West):

Table 2: Convictions for computer crimes (1995-1999, old territory of the FRG plus Berlin

East&West)

Year	1995	1996	1997	1998	1999
Computer fraud (§ 263a)	1541	1742	1980	2470	2157
alteration of data (§ 303a)	7	5	10	4	4
computer sabotage (§ 303b)	1	1	0	0	1
data spying (§ 202a)	1	7	8	4	3

[Rz 6] Even if the data in Table 2 are not directly comparable to the data in Table 1 (because the latter include the new states), it becomes very clear that only a few cases that are known to the police result in a court conviction. Additionally, one has to keep in mind that in the case of computer fraud (§ 263a Penal Code) most sentences are not related to Internet-activities (e.g. credit card manipulations, 0190-Dialer, manipulation of gambling machines etc.). Obviously, the criminal justice system is facing a serious implementation problem in the area of Internet criminality. This is mirrored by the fact that only a very few court decisions are related to alteration of data (§ 303a Penal Code), computer sabotage (§ 303b Penal Code), or data spying (§ 202a Penal Code) are published in the literature.

I. Criminal provisions against computer viruses

1. Damaging data by virus programs

a) Dogmatic analysis of §§ 303a, 303b StGB

> *German Penal Code, § 303a - Alteration of data*
>
> *(1) Anybody who unlawfully deletes, suppresses, renders unusable, or alters data (§ 202a subsection 2), shall be punished with imprisonment not exceeding 2 years or a fine.*
>
> *(2) The attempt shall be punishable.*
>
> *German Penal Code, § 303b - Computer sabotage*
>
> *(1) Anybody who interferes with a data processing activity which is of vital importance to the business or enterprise of another or a public authority by*
> *1. committing an offence under § 303a subsection 1 or*
> *2. destroying, damaging, rendering unusable, removing or altering a data processing system or carrier shall be punished with imprisonment not exceeding five years or a fine.*
>
> *(2) The attempt shall be punishable.*
>
> *German Penal Code, § 303c - Request for prosecution*
>
> *Offences referred to in §§ 303 to 303b shall be prosecuted only on request except where the prosecutorial authority, in view of the particular public interest involved, deems that ex officio action is required.*

[Rz 7] § 303a Penal Code — The **legal interest** [Rechtsgut] protected by this provision is the "unimpaired disposability of data by the right holder", i.e. others are excluded from the utilisation of that data without consent of the right holder (consequently, the right holder's data and information are protected by the Penal Law).

[Rz 8] The Penal Code does not comprise a definition of the term " **data**". The term has to be understood in a wide sense as a sequence of signs or signals that have informative value

(information translated into code). This also includes computer programs. § 202a Subsection (2) contains a restriction to data stored or transmitted electronically, magnetically, or in any other not directly perceptible way, which is relevant for §§ 202a Subsection (1), 269, 274 Subsection (1) No. 2, 303a.

[Rz 9] Dogmatically, it is unclear how the **right holder of the data** can be determined. Property law does not apply; neither can the right holder of the data be equated with the right holder of the data-storing device. The disposability of data can arise from a copyright or a derivative ownership. If, for example, the original right holder sends a digital copy of the data to a third person giving him a right to use the document, that person is entitled to dispose of the data in her own right (see Kühl – in: Lackner/Kühl 2001, § 303a N 4).

[Rz 10] The **incriminated acts** are:

- Deletion = to render specific data and the information contained therein completely and irretrievably unrecognisable
- Suppression, rendering unusable, alteration = the disposability can also be impaired by making the data unaccessible for a certain (considerable) time, like in the case of DoS attacks, and by making changes to the content of a data file.
- If a person has a legal duty to protect the data [Garantenstellung], the incriminated acts can also be committed by omission.

[Rz 11] In Internet-related cases, the alteration of data can take place both in the course of the data transfer and when the data are stored on a computer connected to the Internet. § 303a Penal Code applies to both cases.

[Rz 12] § 303b Penal Code — Computer sabotage is a special case of data alteration [qualifizierter Tatbestand] and results in a more severe punishment. The provision aims to protect data processing units like single computers network computers (servers), or mainframe computers of businesses or enterprises. Only if the data processing function of the computer is of **vital importance for a business or enterprise**, § 303b Subsection (1) No. 1 applies instead of § 303a Penal Code. This is the case when the daily operations of a company depend on the undisturbed functioning of electronic data processing (tax calculation, salary records etc.).

[Rz 13] It is disputed whether § 303b Subsection (1) No. 2 only applies, if the data processing unit or some data storing device is physically damaged, or whether it applies also to the implantation of a computer virus program. If the virus has direct damaging effects on the computer hardware this can be admitted (see Fischer – in: Tröndle/Fischer 2001, § 303b N 7).

[Rz 14] Criminal prosecution is dependent on a complaint filed by the right holder. In exceptional cases where public interests are affected, ex officio action by the public prosecutor is possible (§ 303c Penal Code).

b) Court decisions

[Rz 15] **Killer programs** – LG Ulm, 1. Strafkammer - Entscheidung vom 1.12.1988
The installation of so-called killer programs that render a software unusable after a specific date is punishable according to §§ 303a, 303b Penal Code.
Source: Computer und Recht 1989, 825 – 826

[Rz 16] **Hacker Kimbel case** – LG München I - Entscheidung vom 23.3.1998 – AZ: 6 KLs 315 Js 18225/ 94
Facts: Two defendants – known as “Kimble” and “Big Trumbler” in hacker circles – agreed around the end of 1992 to use safety holes in the computer systems of larger companies to intrude into these systems. The intrusions were documented and later used to convince the same companies to buy a data protection tool produced by Fast Comtec (a company owned by a member of the defendants’ hacker group). Conspiring with other offenders, they planned to

intrude into the Norwegian Data-Pak-network and to record so-called NUI's (National User Identification). Using these identifications, they intended to get into the Datex-P-network of Deutsche Telekom to spy on all Datex-P-connections of larger companies. Defendants planned to transfer all capture-files of these unauthorised intrusions to a network security company called Infosafe, which was established by fellow hackers. Infosafe would then approach these companies to offer safety tools. The defendants were linked to Infosafe by a counsellor agreement, which entitled them to receive an advance fee of DM 20 000.- and a monthly honorarium of DM 6 500.- (under certain conditions). In total, the defendants received DM 131 000.- from Infosafe. To save telephone fees, the defendants used illegally obtained calling-card numbers of AT & T clients and connected through this channel to the Data-Pak-network "free of charge". The damage had to be covered by AT & T. By this method, the defendants succeeded at least twice in intruding into the password protected computer systems of companies connected to the Datex-P-network and were able to copy internal data (e.g. the correspondence of the German civil servants' Association with the German Chancellor). Part of the information was disseminated to a weekly journal. The indictment cites additional charges, which are not related to network crimes (e.g. credit card fraud, unauthorised use of calling cards).

[Rz 17] Decision: The defendants were found guilty of conspiracy in computer fraud (§ 263a Penal Code) on 8 accounts, data spying (§ 202a Penal Code), treason of business and trade secrets (§§ 17 Subsection 2 No. 1a, 22 Unfair Competition Law) and other offences (not related to the unauthorised access to computer systems). "Kimble" was sentenced to two years of juvenile punishment [= imprisonment, Jugendstrafe] suspended for a probationary period [auf Bewährung]. "Big Trumbler" was sentenced to two years of imprisonment suspended for a probationary period [auf Bewährung].

[Rz 18] Reasons: The District Court made clear that spying on data that are specially secured against unauthorised access and that are not meant for the offender is an infringement of § 202a Penal Code. Instead, simple intrusion without retrieval of protected data remains beyond the range of the provision, i.e. is not punishable. If the intruder damages data on the computer system of another or if he alters it, alteration of data (§ 303a Penal Code) or computer sabotage (§ 303b Penal Code) sections are applicable.
Source: Computer und Recht International 1998, 209
Online-source: http://www.kimschmutz.de/kimble/die_akte_kim_schmitz.txt

[Rz 19] **Mixter case** – LG Hannover – Entscheidung vom 31.3.2000 – AZ: 31 b 11/00 (revision at the juvenile court)
Facts: At the age of 19 years, the defendant – known as "Mixter" in hacker circles – intruded repeatedly into the computer system of a company. There, he installed computer virus programs and spied on data. The material damage was estimated at DM 34 000.-.

[Rz 20] Decision: the defendant was found guilty of computer sabotage (§ 303b Penal Code) on 8 accounts and of data spying (§ 202a Penal Code). He was sentenced to six months of juvenile punishment [= imprisonment, Jugendstrafe] suspended for a probationary period of two years [auf Bewährung]. At first instance [Amtsgericht] the defendant was sentenced to 15 days of community service. The Juvenile Prosecutor filed an appeal against this ruling.

[Rz 21] Reasons: The District Court found that the material and immaterial damage caused by the computer sabotage of Mixter was such that a community service order would not suffice to prevent him from future serious hacking attacks.

[Rz 22] Comment: Mixter, who is 22 years old now, became famous for his "Tribe Flood Network" program, which was used in the Denial of Service Attacks against yahoo.com, CNN.com, ebay.com etc. in early 2000.
Online-source: http://www.chip.de/news_stories/news_stories_65821.html

[Rz 23] Computer virus programs have also been subject to some **civil law litigation**.

[Rz 24] Herbstlaubvirus – Regional Labour Court Saarland, 1 December 1993 (infection of the employer's computer system regarded as important reason for immediate dismissal; the court left open whether §§ 303a, 303b Penal Code were applicable)
Source: Computer & Recht 1994, 296 – 301 and JurPC 1995, 3151 – 3166

[Rz 25] Contractual liability for virus on a floppy disk – Regional Court Hamburg 18 July 2001 (if a contract includes the duty to check floppy disks for computer viruses, the supplier can be held liable to pay damages, also for consequential harm caused by the defective disk)
Online-source: http://www.jurpc.de/rechtspr/20010193.htm

2. No provisions against the production, distribution etc. of computer virus programs

[Rz 26] The German Penal Code does not contain any provision that makes the production, distribution or making accessible of computer virus programs a crime. Neither is there such provision regarding giving instructions to aid the production of such programs.

[Rz 27] In the literature, some authors want to treat such acts as aiding & abetting [Beihilfe] in the sense of § 27 Penal Code (see Jaeger 1998). Others propose that posting a computer virus kit on a WebPages for downloads or making it accessible in other ways could be punishable as incitement [Anstiftung, § 26 Penal Code] to a crime in the sense of §§ 303a, 303b Penal Code (see Preuße 2001, 125 et seq.). This solution is only justifiable, if the offender, who incites, acts with premeditation to incite a duly identifiable person. If, however, the offender's stimulus is directed towards an uncontrollable and unrecognisable subgroup of persons – as is most often the case – the condition of a "specific concretion" of the incitement [bestimmter Konkretisierungsgrad] is lacking.

II. Lack of criminal provision against illegal access to computer systems (hacking)

a) Dogmatic analysis of § 202a StGB

> *German Penal Code, § 202a - Data spying*
>
> *(1) Anybody who without authorisation procures for himself or another person data, which are not meant for him and which are specially secured against unauthorised access, shall be punished with imprisonment for not more than three years or a fine.*
>
> *(2) Data within the meaning of subsection (1) shall be deemed to be only those which are stored or transmitted electronically, magnetically, or in any other not directly perceptible way.*
>
> *German Penal Code, § 205 - Request for prosecution*
>
> *(1) Offences referred to in § 201 subsection (1) and (2) and in §§ 202 to 204 shall be prosecuted only on request.*
>
> *(2) … [Provision regulating who can exercise the right to file a request for prosecution if the right holder has deceases]*

[Rz 28] The **legal interest** [Rechtsgut] protected by this provision is the "formal right to disposability"; i.e. the right holder has a right to determine who has access to the information contained in the data. The Penal Code, hence, protects the interest of the right holder in the secrecy of the data. The data need not necessarily be a secret; § 202a Penal Code applies in all cases where the right holder has not consented in the reading by the other (**formal secrecy**). § 202a Penal Code protects all data, even data with no property value [Vermögenswert, note that there is no precise term in English for "Vermögen" as opposed to "Eigentum"].

[Rz 29] For a definition of the term **data**, see above (A.I.1.a).

[Rz 30] The data may **not be meant for the offender**, i.e. he or she does not have the consent of the right holder to access the data. Furthermore, the data must be **specially secured against unauthorised access**. Because the data have no physical appearance, they often cannot be protected by physical means like keys, boxes etc. (except for cases where the data is stored on a removable disk or the computer is not connected to a network). Thus, a special protection can be assumed, if measures have been taken that are objectively suitable to exclude or at least to render more difficult the access by others to the data of the right holder. Subjectively, the right holder must use the protection with a will to exclude others; i.e. the interest to keep the (formal) data secret must be recognisable. However, a symbolic protection measure is not adequate; it must be an effective protection. Whether a protection measure is regarded as effective or not, depends on the individual circumstances. For example, during the delivery of a simple e-mail over the Internet, the data are not specially protected. If the sender uses **cryptography software** to encode the data prior to sending them, the criteria of special protection is certainly met. Although the offender still may spy on the data, he or she cannot access the information content right away (but only after decrypting the data file).

[Rz 31] The **incriminated act** is defined as procuring data for the advantage of oneself or another. This means that the control over the information must shift to the offender, but it needn't necessarily lead to a complete loss of control on the side of the right holder. In the digital data world, copies of data files can be easily produced. Accordingly, the incriminated act is already completed, when the control over the information is enlarged without consent of the right holder.

[Rz 32] Spying on or procuring data can take place in two distinct ways:

- Data can be procured **without any conscious electronic copying**, by simply reading it on a computer screen after retrieving it from a specially secured data storage device (e.g. a local harddisk, a mail-server etc.). The literature makes a difference between simple, transitory perception (which does not fall under § 202a Penal Code) and reliable, useable perception (which is punishable under § 202a Penal Code). Put simply, if the offender has memorised the information contained in the data, he or she has completed the incriminating procurement (see Binder 1995, 60; Fischer – in: Tröndle/Fischer 2001, § 202a N 9; some authors refute this interpretation, see Hauptmann 1989, 217).
- Data can also be procured by **consciously producing a copy** (e.g. making a copy of the data file on a floppy disk, the offender's own harddisk etc.). In such cases the offender gets permanent control over the data. Hence, the simple fact of copying is enough to complete the crime (i.e. no specific perception is required because the offender has control over the data at leisure). The only exception is cryptographically encoded data.

[Rz 33] The question whether the illegal access to a computer system without any data alteration or computer sabotage – usually referred to as **hacking** – is punishable under § 202a Penal Code is hotly disputed. The majority of the literature answers in the negative (see Kühl - in: Lackner/Kühl 2001, § 202a N 5; Lenckner - in: Schönke/Schröder 2001, § 202a, N 10). This is explained with an explicit statement in the legislative report on the revision of the Penal Code in 1986 (BT-Dr. 10/5058, 28), which says that merely intruding into a computer system without authorisation was not punishable.

[Rz 34] The wording of § 202a Penal Code lends itself also to a different interpretation. As has been said, committing information contained in a certain data file to memory implies already a procurement of data. Now, upon successfully overcoming the specific protection of a computer system, the hacker automatically gets to know messages from the computer's operation system. If the perceived data contain information (e.g. a password, a file directory, a list of the stored mails etc.), and the hacker memorises it, the intrusion would include a procurement of data and, thus, fit the definition given above (Sieber 2000; see the analysis of Preuße 2001, 88 et seq., the author holds that simple intrusion is not punishable). There is, as yet, no case-law on this particular

topic. If data files are opened (e.g. e-mail, data sheet, text etc.) and memorised or copied, §202a Penal Code applies in any case.

[Rz 35] In Internet-related cases, the data spying can take place both in the course of the data transfer and when the data are stored on a computer connected to the Internet. § 202a Penal Code applies to both cases.

[Rz 36] Criminal prosecution is dependent on a complaint filed by the right holder (§ 205 Subsection 1 Penal Code).

[Rz 37] Hacker Kimbel case – LG München I - Entscheidung vom 23.3.1998 – AZ: 6 KLs 315 Js 18225/ 94 (see above, A.I.1.b)

[Rz 38] Mixter case – LG Hannover – Entscheidung vom 31.3.2000 – AZ: 31 b 11/00 (revision at the juvenile court) (see above, A.I.1.b)

III. Projects for revision

[Rz 39] In a recently issued report to the parliament, the Federal government concluded that there is no immediate need for a revision of the Penal Code provisions related to computer crimes. It stated that the international developments will be carefully studied; this will eventually lead to amendments to the Penal Code (especially regarding the illegal access to computer systems, see Deutsche Bundesregierung 2001, 27 et seq.).

[Rz 40] The Federal Ministry of Justice answered our inquiry as follows:
The adaptation of the German Penal Code to the new provisions of the Cybercrime Convention is not yet envisaged. It is not clear whether § 202a Penal Code has to be changed because the Cybercrime Convention permits member states to make several restrictions. Before ratification can take place, it is essential that Austria, Switzerland and Germany produce a concerted translation into German language.

B. Switzerland

[Rz 41] Several provisions, which have been added to the Penal Code in 1995 (see BBl 1991 II 969), cover the field of computer crimes: Unauthorised procurement of data (Art. 143 Penal Code), unauthorised intrusion into a data processing system (Art. 143bis Penal Code), damaging of data (Art. 144bis No. 1 Penal Code), production, distribution etc. of computer virus programs (Art. 144bis No. 2 Penal Code), fraudulent abuse of a data processing unit (Art. 147 Penal Code), exploitation of a service (Art. 150 Penal Code), forgery of documents (data documents, Art. 251 No. 1, 110 No. 5 Penal Code) and others.

[Rz 42] The national Police Statistics do not yet include separate data categories for computer crimes, therefore, only court statistics can be presented here:

Table 3: Convictions for computer crimes (1995-1999)

Year	1995	1996	1997	1998	1999
unauthorised procurement of data (Art. 143)	1	2	2	2	3
unauthorised intrusion into a data processing system (Art. 143bis)	0	1	0	1	1
damaging of data (Art. 144bis No. 1)	13	17	na	20	8
Production etc. of computer virus programs (Art. 144bis No. 2)	1	0	na	2	1
Fraudulent abuse of data processing unit (Art. 147)	52	224	368	394	396

[Rz 43] A similar picture like in Table 2 for Germany emerges for Switzerland. There are very few cases of computer crimes that reach the level of court proceedings and adjudication. In the category of "computer fraud" it can be presumed that most cases are not carried out via Internet. Compared to an increasing number of media reports about cybercrime and survey results that show how often businesses are affected by hacker activities and computer viruses (see KPMG 2001), these results reflect the difficulties of law enforcement authorities in combating cybercriminals.

I. Criminal provisions against computer viruses

1. Damaging data by virus programs

a) Dogmatic analysis of Art. 144bis No. 1 StGB

> *Swiss Penal Code, Art. 144bis - Damaging of data*
>
> *1. Anyone, who without authorisation modifies, deletes, or renders unusable electronically or similarly saved or transmitted data, will, if a complaint is filed, be punished with imprisonment [Gefängnis = up to 3 years] or a fine [Busse = up to 40 000.- Swiss francs].*
>
> *If the offender has caused a large damage, imprisonment [Zuchthaus] of up to 5 years is possible. The crime will be prosecuted ex officio.*
>
> *2. Anyone, who creates, imports, distributes, promotes, offers, or makes accessible in any way programs, that he/she knows or ought to assume that it will be used for purposes according to item 1 listed above, or gives instructions to create such programs, will be punished with imprisonment [Gefängnis = up to 3 years] or a fine [Busse = up to 40 000.- Swiss francs].*
>
> *If the offender acts for profit, imprisonment [Zuchthaus] up to 5 years is possible.*

[Rz 44] Art. 144bis No. 1 Penal Code is similar to the German § 303a Penal Code. The **legal interest** [Rechtsgut] protected by this provision is also the "unimpaired disposability of data by the right holder". The provision is classified as a "Property Crime" [Vermögensdelikt], but the data are not supposed to have an economical value.

[Rz 45] The Swiss Penal Code does not define the term " **data**". From the legislative report it becomes apparent that both non-executable data like text, image, sound, or source codes, and program files are included (contrary to terminology in computer science). In order to distinguish data from physical objects, the definition only refers to codified, non-visually perceivable data. Art. 144bis No. 1 Penal Code only protects **electronically** or **similarly saved** or **transmitted** data, which requires a "higher level" computer system. The legislator wanted to exclude cash registers, cigarette/beverage/ticket vending machines, slot/gambling machines, if they are not directly connected to a computer system. If such machines (automats) are manipulated, theft (Art.

139 Penal Code), exploitation of a service (Art. 150 Penal Code) or interference with a service, which serves the public (Art. 239 Penal Code) apply (see Schmid 1994, § 2 N 19).

[Rz 46] **Right holder of the data** can be the creator of the data or somebody who has acquired the immaterial property right or a right to use. There can be more than one right holder at the same time (disposing over several copies of the data). If the information contained in the data is about a person, this person is normally not a right holder in the sense of Art. 144bis No. 1 Penal Code (e.g. a client profile, which has been collected by an e-commerce provider, does not give the recorded client a right in the sense of Art. 144bis No. 1 Penal Code).

[Rz 47] There are only three **incriminated acts** (compared to four in Germany and Austria). The suppression of data has been excluded from the usual list. This normally renders the provision inapplicable to denial of service attacks (DoSA) because such attacks neither alter, delete or render unusable the data itself (see Schwarzenegger 2001).

[Rz 48] "Alteration" and "deletion" are manipulations directed against the data itself, whereas "rendering unusable," means a change in the logical access to the data. The damage created by the act must have a certain significance (e.g. inserting only a word to a text file is not regarded as "alteration" in the sense of Art. 144bis No. 1 Penal Code) and must be irreversible. As a general rule, the infiltration of a computer virus program can be interpreted as an "alteration". This is true for computer viruses that attach themselves to a data file of software; however, there are types of computer viruses that "only" settle down in the harddisk without significant damage to the data files thereon.

[Rz 49] Often, computer virus programs are distributed through e-mail-attachments, which require the user to activate the attached file. Strictly speaking, the receiver initiates the damaging process by himself/herself. Nevertheless, the distributor of the computer virus is regarded as **indirect offender** [mittelbarer Täter], as long as the receiver who starts the damaging process did not know the consequences of his or her action.

[Rz 50] In Internet-related cases, the damaging of data can take place both in the course of the data transfer and when the data are stored on a computer connected to the Internet.
Criminal prosecution is dependent on a complaint filed by the right holder. If the damage caused is over sfr. 10 000.- the crime will be prosecuted ex officio (Art. 144bis No. 1 Subsection 2 Penal Code).

b) Court decisions

[Rz 51] **Arsène Z.** — Order of summary punishment by the Prosecution Judge of Vaud, 31 March 1999 (see below, B.II.2)

2. Production, distribution etc. of computer virus programs (Art. 144bis No. 2 StGB)

a) Dogmatic analysis of Art. 144bis No. 2 StGB

[Rz 52] This provision aims to prevent the damaging of data at an early stage by criminalising specific preparatory activities. Accordingly, there needn't be an actual risk for a data file; just performing one of the incriminated acts is enough to be punishable. In Swiss and German penal doctrine, such crimes are called **abstract risk crimes** [abstrakte Gefährdungsdelikte].

[Rz 53] Art. 144bis No. 2 Subsection 1 StGB mentions virus programs "that the offender knows or ough to assume that it will be used for purposes according to item 1" of Art. 144bis No. 1 StGB. A question arising from this expression is, whether the virus program must be **self-reproducing** or not. Some authors say this is required (Stratenwerth 2000, § 14 N 64), others contend that this is not necessary (Schmid 1994, § 6 N 52-53; Rehberg/Schmid 1997, 161). At the moment, it is unclear, whether Trojan horses that infiltrate the central storage area of the harddisk without self-reproductive and damaging effects, can be subsumed under Art. 144bis No. 2

Subsection 1 StGB. **Source codes** for computer virus programs are not programs in the sense of Art. 144bis No. 2 Subsection 1 StGB.

[Rz 54] The provision defines a series of **incriminated acts**:

- Creation, import, distribution, promotion, offer, making accessible: A computer virus program is created as soon as it is compiled and linked, i.e. transferred into a machine-readable version (Schmid 1994, § 6 N 56). As a supplementary requirement one should add that the program must be operational, otherwise there is not even an abstract risk for the data (this case could be interpreted as attempt, Art. 21-22 Penal Code). One of the most important versions in this group is "making accessible", which is completed in the event that another person can gain disposability over the program.
- Giving instructions to create such programs: This notion has far reaching consequences. Taken literally, it can be accomplished by lectures at the university or during conference speeches, in which source codes and virus program tools are explained (Schmid 1994, § 6 N 62). In my opinion, a restriction must be made to keep the provision in line with the constitutionally guaranteed freedom of science (see below).
- Possession and purchase of virus programs: Art. 144bis No. 2 Subsection 1 StGB does not include these acts, therefore, they are not punishable.

[Rz 55] Subjectively, the offender must act with premeditation [Vorsatz]. Additionally, he or she must intend that the program will be used for data damaging purposes.

b) Court decisions

[Rz 56] **Hacker-CD-ROM I & II** — Decision by the District Court of Zürich, 20 July 2000, and the High Court of Zürich, 22 February 2001
Facts: The defendant ordered the production of 3 000 copies of a CD-ROM called "Group 42 Sells Out" that he offered for sfr. 70.- through various channels, especially Newsgroups' postings, and distributed for free among media journalists. He sold around 100 copies. The CD-ROM contained an HTML document, which was readable with a Web-browser. Among other information it also contained textfiles and software related to computer viruses. There were no compiled [i.e. machine-readable] virus programs on the CD-ROM. However, it contained source codes of computer virus programs and descriptions for their creation. The defendant did not write these programs by himself. He licensed the product from a US maker that distributed the same CD-ROM overseas. The defendant did not care about the eventual use of these programs by his clients.

[Rz 57] Decision: The defendant was found guilty of damaging data for profit in the sense of Art. 144bis No. 2 Subsection 1 (giving instructions) and Subsection 2 (acting for profit). He was sentenced to a fine of sfr. 300.- and an order was made that the confiscated CD-ROM be destroyed.

[Rz 58] Reasons: The court first clarified the legal term of "computer virus program" (at 1.2). These are "computer programs with the specific function of causing modifications and distructions of data within a computer system. Regularly, these programs are characterised by their ability to self-reproduce. However, also other computer programs – without infecting effects – which aim to damage the data of third parties, fall under the range of Art. 144bis No. 2 Penal Code, like Trojan horses, spoofing programs, salami-tactics, logic bombs, trap doors, worms (with their sub-groups of chain-letters or Christmas-programs)."

[Rz 59] Next, it points out that the only action element objectively called for by Art. 144bis No. 2 Penal Code is the performance of one of the activities described (i.e. to create, import, distribute, promote, offer, or make accessible or to give instructions). It is not necessary that such programs be actually used by anybody (at 1.2).

[Rz 60] On the subjective side, the offender must act with premeditation [Vorsatz] regarding the objective elements of the crime and with intent [Absicht] that the programs shall be used [according to Swiss penal doctrine, the premeditation is assumed, if the offender knew what he was doing and what effects this possibly could cause, and if he acted regardless of the consequences = Eventualvorsatz, the same applies mutatis mutandis for the intent = Eventualabsicht].

[Rz 61] At 1.4 the Court holds that the source codes and auxiliary programs for the creation of virus programs were not yet virus programs in the sense of Art. 144bis No. 2 Subsection 1 Penal Code. Only machine-readable virus programs (compiled programs) can have the data damaging effects that are required by this provision. Therefore, the defendant did not create, offer, or distribute such programs.

[Rz 62] Nonetheless, there is another criminal activity covered by Art. 144bis No. 2 Subsection 1 Penal Code that requires further analysis: giving instructions to create such programs [zu ihrer Herstellung Anleitung geben].

[Rz 63] At 1.5 the Court interprets this term as including acts of incitement and aiding & abetting. In other words, what is normally defined as an inferior contribution to the crime (see Art. 24 and 25 Penal Code) is regarded in this context as a full and independent criminal responsibility. The Court then concludes that defendant by distributing the above mentioned CD-ROM has given instructions to create virus programs.

[Rz 64] At 1.6 the Court affirms that the defendant had criminal premeditation and acted with the intent that others can and will use these programs to damage data of third parties.

[Rz 65] At 2.3 it rejects the defendant's claim that he was being treated unequally under constitutional law (Art. 8 Swiss Constitution), because other persons offering similar computer virus tools were not criminally prosecuted in the past.

[Rz 66] At 3 the Court, additionally, finds that the defendant acted for profit (Art. 144bis No. 2 Subsection 2 Penal Code).

[Rz 67] Finally, at 5.3 the Court partially accepts the defendant's argument that he acted in ignorance of the law (Rechtsirrtum, Art. 20 Penal Code). The evidence presented by the defence showed that computer virus tools and instructions are widely available, online and even in local bookshops. The defendant was probably unconscious of the criminal nature of his action. However, the Court concludes that defendant could have consulted with the authorities or other experts and, thus, prevented this ignorance of the law. His guilt was reduced, but not eliminated by this fact.
Source:
sic! [Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht] 2000, 723 – 727
SJZ [Schweizerische Juristen-Zeitung] Vol. 96 (2000), 511 – 514

[Rz 68] The defendant's **appeal** was rejected by the High Court. At 3.1 the High Court -- contrary to the District Court -- holds that a computer virus program must be self-reproducing. The appeal by the state prosecutor was heard (no ignorance of the law). Thus, the High Court augmented the sentence to two months of imprisonment [Gefängnis] suspended for a probationary period [bedingter Strafvollzug] and a fine of sfr. 5 000.-. The appeal to the Cantonal Cassation Court was successful on procedural grounds. The case is pending for retrial at the High Court.
Source:
sic! [Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht] 2001, 540 – 548
ZR [Blätter für Zürcherische Rechtsprechung] Vol. 100 (2001), 142 – 149

[Rz 69] Personal comment: Both decisions claim that a distinction has to be made between source codes for computer virus programs and the compiled, machine-readable versions of virus programs. Only the latter fall under Art. 144bis No. 2 Subsection 1 Penal Code. However, the

distribution of such source codes and virus construction tools can be understood as "giving instructions to create such programs", which is also punishable. Both courts did not discuss the fact that the instructions have been written by the US maker of the CD-ROM and not by the defendant. Is a person who makes a copy of an instruction and transmits it to others "giving instructions" (by himself/herself as principal perpetrator) or is he/she merely helping the principal perpetrator (conspiracy)? In my view, the courts are not correct in assuming a principal responsibility in all cases of "giving instructions". Principal criminal responsibility can only be admitted, if the defendant by word or deed documents his willingness to distribute the information as his own information (Zueigenmachen).

[Rz 70] Because the subjective elements (intent, purpose) of the provision are assumed if only the offender knows what could happen, the range of application of Art. 144bis No. 2 Subsection 1 Penal Code is very broad. Even a professor teaching computer sciences at the University must anticipate that some of his students might use such knowledge for the production of computer viruses and, therefore, be held criminally liable. In my view, this is an unconstitutional restriction of the freedom of science (Art. 20 Swiss Constitution). Consequently, a restrictive interpretation in light of the constitutional guarantee must be found. One solution could be to limit the subjective element of Art. 144bis No. 2 Subsection 1 Penal Code to direct intention (direkte Absicht, dolus directus ersten Grades). The High Court of Zürich, however, rejected this limiting interpretation (at 5.2).

3. Unauthorised procurement of data (Art. 143 StGB)

> *Swiss Penal Code, Art. 143 – Unauthorised procurement of data*
>
> *Anyone, who with intent to enrich himself or another procures for himself or another electronically or similarly saved or transmitted data, which are not meant for him and which are specially secured against his unauthorised access, will be punished with imprisonment of up to 5 years [Zuchthaus] or imprisonment [Gefängnis = up to 3 years].*
>
> *The unauthorised procurement of data to the disadvantage of [the offender's] relations or family members will only be prosecuted upon complaint.*

[Rz 71] Contrary to the German § 202a Penal Code, Art. 143 of the Swiss Penal Code is closely linked to the category of property crimes. Regarding the legally **protected interest**, Schmid (1994, § 4 N 14 et seq.) contends that Art. 143 is mainly protecting the right holder in his or her "property" [Vermögen], and secondarily, his or her "data secret". Because of this legislative misconception, Art. 143 Penal Code is restricted to cases where the offender acts with intent to illegally enrich himself or another.

[Rz 72] The other elements of the crime (data, "not meant for him", "specially secured against his unauthorised access") are interpreted in the same way as in § 202a German Penal Code (see above at A.II.).

[Rz 73] It is unclear, whether the simple reading of the data satisfies the requirement of "procuring", or whether a copy must be made on a storage device, which is controlled by the offender (see on that question Trechsel 1997, Art. 143 N 7).

[Rz 74] In sum, if a hacker "steals" data from another computer system without authorisation, it is only a crime in the sense of Art. 143 Penal Code if he acts with the intention to enrich himself or another. If the offender acts without such intention, which is most often the case with hackers, only Art. 143bis Penal Code can be applied (e.g. the WEF-hack).

[Rz 75] There is a special case of illegal procurement of data: **Violation of manufacturing and business secrets** (Art. 6 Unfair Competition Law). If such secrets are procured online (with or without intent for enrichment), the offender can be punished according to Art. 6 and Art. 23 of the Unfair Competition Law (if a complaint is filed by the injured party).

II. Criminal provisions against illegal access to computer systems

1. Dogmatic analysis of Art. 143bis StGB

> *Swiss Penal Code, Art. 143bis – Unauthorised intrusion into a data processing system*
>
> *Anyone, who without intent to enrich him or herself by way of data transmission equipments intrudes without authorisation into someone else's data processing system, which is specially secured against his access, will, if a complaint is filed, be punished with imprisonment [Gefängnis = up to 3 years] or a fine [Busse = up to 40000 Swiss francs].*

[Rz 76] Art. 143bis StGB was introduced as an "anti-hacker" provision into the Penal Code. The **legal interest** [Rechtsgut] protected by this provision can be described as the "privacy of the data processing system" that is specially secured against unauthorised access (see Trechsel 1997, Art. 143bis N 2). The categorisation with the chapter of "property crimes" [Vermögensdelikt], thus, is wrong.

[Rz 77] The offensive act is directed against a **data processing system**, which can be a single-user or multi-user computer, instead, not a floppy disk and not the data on their transfer from one data processing system to the other.

[Rz 78] The data processing system must be **someone else's** [fremd], i.e. the offender may not have the right to access the data.

[Rz 79] A special protection can be assumed, if measures have been taken that are objectively suitable to exclude or at least to render more difficult the access by others to the data processing system.

[Rz 80] The **incriminated act** is the intrusion itself, which means the overcoming of the security measures and having access to the system level of the computer.

[Rz 81] Subjectively, the offender must act with premeditation [Vorsatz], but needn't have the intention to enrich himself. The legislator made a mistake because according to the present regulation somebody who acts with the intent to enrichment may not be punished according to Art. 143bis Penal Code. If the offender intrudes into the data processing system, but does not procure any data, he or she goes unpunished (which is an unanticipated consequence of the current regulation!).

[Rz 82] Criminal prosecution is dependent on a **complaint** filed by the right holder.

2. Court decisions

[Rz 83] **Arsène Z.** — Order of summary punishment by the Prosecution Judge of Vaud, 31 March 1999
Facts: At the beginning of 1998, the defendant, a student at the Federal Polytechnical School in Lausanne, took advantage of a security hole in the computer system of the X SA to circumvent its access protection and to gain unauthorised access to its computer system in Zürich. He gained access to the root directory and succeeded in getting control over several network computers. The defendant installed trap doors, which enabled him to return at will. He also used password sniffers that recorded automatically the keyboard strokes of network users. The defendant examined these records periodically. Using passwords obtained in this manner, he was able to get unauthorised access to other networks, one of which being the network of the University of Zürich. Within the University's network he continued his operations like within the computer system of the X SA. To keep his visits to the systems secret, defendant modified, deactivated, or sometimes deleted

track data.

[Rz 84] Decision: The defendant was found guilty of intrusion into a data processing system without authorisation in the sense of Art. 143bis and of damaging of data in the sense of Art. 144bis No. 1 Subsection 1 Penal Code. He was sentenced to 15 days imprisonment [Gefängnis] suspended for a probationary period [bedingter Strafvollzug] and a fine of sfr. 1 000.-. According to Art. 61 Subsection 1 Penal Code the judge ordered the decision to be published on a Website of the Canton of Vaud for two years.

[Rz 85] Reasons: Being an order of summary punishment [Strafbefehl], which is only possible, if the defendant admits to the crimes, few reasons are given. After stating the provisions of the Penal Code, the judge argues that the criminal conduct has been serious because a company has been afflicted that strongly depends on the confidence clients put into its computer system. Considering that defendant has been less than 20 years of age during the first part of his criminal activities and his best efforts to compensate for the damages caused, the judge alleviated the punishment. Because some students at the Federal Polytechnical School in Lausanne seem to be involved in intense "hacking" activities, the judge observes that there is a public interest for the publication of this judgment in order to prevent students from "hacking".
Online-source: http://cowww.epfl.ch/Arsenez.html

[Rz 86] **WEF-hacker** — The case is still under investigation in the Canton of Berne
Facts: During the winter 2000/2001 the 20 year-old computer hacker D.S., an anti-globalisation protester, acting from his computer in Berne, intruded into the server of the World Economic Forum (WEF), which organises high-level business meetings in Davos on a yearly basis. The WEF server is located in Geneva. According to media reports, D.S. made a portscan at Port 1433 and entered "sa" as user name and a blank password (pressing return), which is the standard configuration of the SQL-Server-Database, Version 7.0. D.S. was then able to access confidential information from the database, including credit card numbers, addresses, e-mail addresses, home and cell phone numbers and passport numbers belonging to business people, government officials, academics and journalists who have attended the World Economic Forum (WEF) over the last three years (e.g. Bill Clinton, Bill Gates, Yasser Arafat and many others). D.S. copied these data files and recorded it on a CD-ROM, which he sent for free to the "Sonntagszeitung", a weekly Sunday newspaper.

[Rz 87] Personal comment: The case is interesting in many respects. Firstly, it has been discussed, whether the WEF-server was sufficiently protected against illegal access. The standard configuration of the protection mechanism is generally known (at least in hacker circles), therefore, it can be argued that no such protection was made. Hence, the act would not be punishable at all. A majority of commentators also said that a port-scan would not be punishable under Art. 143bis Penal Code.

[Rz 88] Secondly, the case was investigated in Geneva first, but after it was learned that the suspect lived in Berne, the case was transferred to Berne because the venue for the prosecution lies primarily where the offender has committed the criminal act (Art. 346 Penal Code). No indictment has been issued as of yet.

[Rz 89] Thirdly, in my personal view, it has been completely ignored by the authorities and the media that Art. 6 and Art. 23 of the Unfair Competition Law apply to this case because a business secret has been illegally distributed. These provisions do not require intent to enrich or a special protection of the data.
Online-source: http://money.cnn.com/2001/02/05/europe/standard_wef/
http://www.woz.ch/wozhomepage/davos/micr11j01.htm (in German, on technical details)

III. Projects for revision

[Rz 90] According to the Report on State Defence issued by the Federal Police one focus of

activities lies in the field of violent extremism and racist propaganda on the Internet. A contact group between federal authorities and various national ISP has been established to discuss legal and technical preventive measures, including the blockade of criminal websites, international co-operation and self-control by ISP (see Staatsschutzbericht 1998, 143).

[Rz 91] The Federal Ministry of Justice answered our inquiry as follows:
Switzerland has signed the Cybercrime Convention on November 23, 2001. Before ratification can take place, several changes to the national legal system are necessary, especially, a 7/24 contact point has to be established first. We expect that this contact point as well as the new monitoring office will be established within the Federal Police Office in Berne. Since 1 April 2002 the range of Art. 197 Penal Code has been extended. Possession of child pornography (and other forms of hard pornography) is now a crime punishable with up to 1 year imprisonment. In the framework of the current works on a Federal Criminal Procedure Code the procedural provisions contained in the Cybercrime Convention are to be discussed. Concerning the distribution of computer viruses and hacking (Art. 143bis and Art. 144bis Penal Code) no revisions are needed.

C. Northern Europe (Scandinavian Countries)

I. Sweden

Penal Code, Chapter 4, Section 9c

A person who, in cases other than those defined in Sections 8 and 9, unlawfully obtains access to a recording for automatic data processing or unlawfully alters or erases or inserts such a recording in a register, shall be sentenced for breach of data secrecy to a fine or imprisonment for at most two years. A recording in this context includes even information that is being processed by electronic or similar means for use with automatic data processing. (Law 1998:206)

[Rz 92] This provision deals with “data trespass”. It can be applied to all kinds of illegal access to computer systems, including many forms of hacking. In the early 1990s a legislative committee put forward a very detailed and innovative proposal for specific criminal law regulations concerning computer crimes. The ministry of justice started working on these proposals for many years, but in the end only few changes were realised (like the inclusion of Chapter 4, Section 9c Penal Code). An English summary of the committee’s proposals is published in Statens offentliga utredningar (1992, 67 et seq.). The Swedish colleagues have reported no major court cases on hacking or computer virus distribution.

[Rz 93] The Swedish government has signed the Cybercrime Convention and is currently studying the need for a revision of the Penal Code.

II. Finland

Penal Code Chapter 38, Section 8: Data trespass (578/1995)

(1) Any person who, by using an identification code that does not belong to him or by breaking through a corresponding protective system unjustifiable, breaks into a computer system where data are processed, stored or transmitted by electronical or other technical methods or into a separately protected part of such a system, shall be sentenced for data trespass to fines or imprisonment not exceeding one year.
(2) For data trespass is also sentenced any person without breaking into a computer system or a part thereof, uses a special technical device to unjustifiably obtain information that is stored in such a computer system.

(3) Attempt is also punishable.
(4) This section will only be applied if the act is not punishable as a more severe offence.

[Rz 94] According to this provision it is illegal to use an unauthorised access code or otherwise break a protection in order to hack unlawfully into a computer system where data is processed, stored or transmitted electronically or in a corresponding technical manner. Furthermore, it is illegal without hacking into the computer system, to use a special technical device to obtain information contained in a computer system. The rationale of these provisions is to protect the computer systems against any unauthorised access. The offender must act with premeditation.

III. Denmark

Penal Code, Section 263

(1) Any person who without authorisation
1. opens a letter, a telegram, or another closed message or record, or withholds it from somebody or takes notice of its content,
2. procures himself access to a closed repository of someone else,
3. secretly intercepts or records statements made in private, telephone conversations or other conversations between any third parties or non-public negotiations, in which he himself does not participate or to which he has procured himself unauthorised access, shall be punished with a fine or imprisonment up to 6 months.
(2) Any person who, in an unlawful manner, obtains access to another persons information or programs which are meant to be used in a data processing system, shall be punished with a fine or imprisonment up to 6 months.
(3) If an act of the kind described in Subsection (1) or (2) is committed with the intent to procure or make oneself acquainted with information concerning trade secrets of a company or under other extraordinarily aggravating circumstances, the punishment can be increased to imprisonment up to 2 years.

Penal Code, Section 291

(1) Any person who, destroys, damages, or conceals things, which belong to another, shall be punished with a fine or to imprisonment up to 1 year.
(2) If damages of a large scale are committed or if the offender has been found guilty of this Section or Sections 180, 181, 183 Subsection (1) and (2), 184 Subsection (1), 193 or 194 before, the punishment can be increased to imprisonment up to 4 years.
(3) If the damage described in Subsection (2) is caused by gross negligence, the punishment is a fine or imprisonment up to 6 months.

[Rz 95] Spreading a computer virus is punishable according to Section 291 Penal Code since the Østre Landsret [High Court] has decided that “things” in the sense of Subsection (1) means also computer programs, decision U 1987.216 Ø).

[Rz 96] Hacking can be punishable under Section 263 Subsection 1 No. 1 or Subsection 2.

Christian Schwarzenegger (www.rwi.unizh.ch/schwarzenegger) is assistant professor of criminal law, criminal procedural law and criminology at the University of Zurich. Furthermore he´s a member of the Swiss Expert Committee for Network Criminality.

Report on behalf of the Expert Committee of the Japanese Ministry of Economy, Trade and Industry (METI, formerly: MITI). The summary report of the Expert Committee has been published in April, 2002 and can be downloaded from (Japanese only): http://www.meti.go.jp/kohosys/press/0002626/. The author would like to thank lic.iur. Stefan Heimgartner and Sarah Summers, LLB (Hons.), for their support in preparing this report.

The report is available in Japanese, see: Saibâ keijihô kenkyûkai hôkokusho, Ôshû hyôgikai saibâ hanzai jôyaku to waga-kuni no taiô ni tsuite, Keizaisangyôshô, 2002-nen 4-gatsu [Report of the Research Committee on Criminal Law in Cyberspace: On the Convention on Cybercrime of the Council of Europe and the corresponding actions of Japan, METI: Tokyo, April 2002]

References:

Binder, Jörg: Computerkriminalität und Datenfernübertragung. Teil I, Recht der Datenverarbeitung 1995, 57 – 60; Teil II, Recht der Datenverarbeitung 1995, 116 - 123
Dannecker, Gerhard: Neuere Entwicklungen im Bereich der Computerkriminalität – Aktuelle Erscheinungsformen und Anforderungen an eine effektive Bekämpfung. Betriebsberater 1996, 1285 – 1294
Deutsche Bundesregierung: Wirksamer Schutz vor Computerattacken (Antwort auf eine Grosse Anfrage). BT-Dr. 14/6321 vom 20.6.2001
Hilgendorf, Eric: Probleme des § 303a StGB - BayObLG, Urteil vom 24. Juni 1993, 5 St RR 5/93. Juristische Rundschau 1994, 478 – 480
Hofer, Thomas: Computer-Viren – Herkunft, Begriff, Eigenschaften, Deliktsformen. JurPC 1991, 1367 – 1374
Jaeger, Stefan: Anbieten von „Hacker-Tools“. Zur Strafbarkeit „neutraler Handlungen“ als Beihilfe. Recht der Datenverarbeitung 1998, 252 - 255
KPMG (ed.): efr@ud.survey. Umfrage zur Wirtschaftskriminalität im eCommerce, 2001, available at: http://www.kpmg.de/library/surveys/
Lackner, Karl / Kühl, Kristian: Strafgesetzbuch mit Erläuterungen. 24. ed. München 2001
Mühle, Kerstin: Hacker und Computerviren im Internet. Eine strafrechtliche Beurteilung. Passau 1998
Preuße, Thomas: Informationsdelikte im Internet. Hamburg 2001
Rehberg, Jörg / Schmid, Niklaus: Strafrecht III. 7. ed. Zürich 1997
Scheffler, Hauke / Dressel, Christian: Die Insuffizienz des Computerstrafrechts. Zeitschrift für Rechtspolitik 2000, 514 – 517
Schmid, Niklaus: Computer- sowie Check- und Kreditkarten-Kriminalität. Zürich 1994
Schmitz, Roland: Ausspähen von Daten, § 202a StGB. Juristische Arbeitsblätter 1995, 478 – 484
Schönke, Adolf/Schröder, Horst: Strafgesetzbuch. Kommentar. 26. ed. München 2001.
Schwarzenegger, Christian: Intaanetto ni okeru keihô no bashoteki tekiyô han’i. Hôgaku Ronshû 1999, 125 - 153
Schwarzenegger, Christian: Der räumliche Geltungsbereich des Strafrechts im Internet, Schweizerische Zeitschrift für Strafrecht 2000, 109 – 130
Schwarzenegger, Christian: E-Commerce – Die strafrechtliche Dimension – in: Alter, Oliver /Jörg Florian (eds.): Internetrecht und E-Commerce-Law. Lachen/St. Gallen 2001.
Schwarzenegger, Christian: Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime vom 23. November 2001. Am Beispiel des Hackings, der unrechtmässigen Datenbeschaffung und der Verletzung des Fernmeldegeheimnisses, in: Donatsch, Andreas / Forster, Marc / Schwarzenegger, Christian (eds.): Strafrecht, Strafprozessrecht und Menschenrechte. Festschrift für Stefan Trechsel zum 65. Geburtstag. Zürich, 2002, 305-324
Sieber, Ulrich: Strafrecht und Strafprozessrecht – in: Hoeren, Thomas/Sieber, Ulrich (Hrsg.): Handbuch Multimedia-Recht, Rechtsfragen des elektronischen Geschäftsverkehrs (Loseblatt), München 2000, 19, 1 – 290
Statens offentliga utredningar, Justitiedepartementet (ed.): Information och den nya InformationsTeknologin – straff – och processrättsliga frågor m.m. Stockholm 1992
Stratenwerth, Günter: Schweizerisches Strafrecht, Besonderer Teil II: Straftaten gegen Gemeininteressen. 5. ed. Bern 2000.
Trechsel, Stefan: Schweizerisches Strafgesetzbuch. Kurzkommentar. 2. ed. Zürich 1997.
Tröndle, Herbert/Fischer, Thomas: Strafgesetzbuch und Nebengesetze. 50. ed. München 2001.

Rechtsgebiet Strafrecht
Erschienen in Jusletter 14. Oktober 2002
Zitiervorschlag Christian Schwarzenegger, Computer crimes in Cyberspace, in: Jusletter 14. Oktober 2002 [Rz]
Internetadresse http://www.weblaw.ch/jusletter/Artikel.jsp?ArticleNr=1957