Lecture Notes in Computer Science 741
Edited by G. Goos and J. Hartmanis

Advisory Board: W. Brauer D. Gries J. Stoer

Series Editors

Gerhard Goos
Universität Karlsruhe
Postfach 69 80
Vincenz-Priessnitz-Straße 1
D-76131 Karlsruhe, Germany

Juris Hartmanis
Cornell University
Department of Computer Science
4130 Upson Hall
Ithaca, NY 14853, USA

Volume Editors

Bart Preneel
René Govaerts
Joos Vandewalle
Departement Elektrotechniek, Katholieke Universiteit Leuven
Kardinaal Mercierlaan 94, B-3001 Heverlee, Belgium

CR Subject Classification (1991): C.2.0, D.4.6, E.3-4, G.2.1, K.6.5

ISBN 3-540-57341-0Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-57341-0 Springer-Verlag New York Berlin Heidelberg

Printed in Germany

Typesetting: Camera-ready by author
Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.
45/3140-543210 - Printed on acid-free paper

Preface

The ESAT Laboratorium of the Department of Electrical Engineering at the Katholieke Universiteit Leuven regularly organizes a course on the state of the art and evolution of computer security and industrial cryptography. The first course took place in 1983, the second in 1989, the third in 1991, and the fourth course is scheduled for 1993.

The ESAT course is intended for both researchers and practitioners from industry and government. It covers the basic principles as well as the most recent developments. Because of our background and because of the relevance, the emphasis lies on cryptography without forgetting the most important topics in computer security. We try to strike the right balance between basic theory and real life applications, between mathematical background and juridical aspects, and between recent technical developments and standardization issues.

During our 1991 course Walter Fumy suggested editing the text of the speakers into more formal written documents. All speakers were invited to submit their contributions, and almost all of them responded positively with an excellent text. We feel that the result – complementary to text books and conference proceedings – can be very interesting for those interested in cryptography and computer security. We would like to thank the authors for their careful preparation of their contributions.

Leuven, Belgium
1993

B.P, R.G, and J.V.

Contents

Section 1

Introduction

Trends in the Fight Against Computer-Related Delinquency

Prof. Dr. B. De Schutter

Director Center for International Criminal Law
Vrije Universiteit Brussel

1 Characteristics of the Phenomenon

The grasp of information technology upon almost all societal activities is an indisputable and irreversible fact. Transfer of data, information, knowledge or know-how has undergone with the technological wave a profound change in its form, speed and distance coverage. This mutative effect can certainly be beneficial to society in all its components (economic, strategic, intellectual, cultural).

It seems, however, that the margin between use and abuse is rather narrow. Even if criminality related to information has always existed, the intervention of the computer with its above-mentioned characteristics of time, volume and place, leads to the risk of a criminal activity, the nature of which might be different from the more classical information crimes. To look into the phenomenon, its size frequency and profile, will lead to the necessary conclusion for the need of policies, which may be necessary to effectively combat this anti-social behaviour.

In that exercise one encounters a number of difficulties. A first one concerns already the definition of computerdelinquency. According to the purpose for which it is needed, one can work with a more criminology-oriented definition, describing the deviant pattern from the sociological angle, or could need a more precise terminology when introducing the illegal act as crime in the penal arena, then requiring precise material and moral elements in the definition. Avoiding the multitude – and the nuances – of definitions of the expert writers [1], there is much merit in the OECD working definition, referring to "any illegal, unethical or unauthorized behaviour relating to the automatic processing and/or the transmission of data" [2], since the answer to computer criminality is likely not to be limited to an exercise of criminal law drafting alone. However, the danger, of such an extensive "opening definition" is that it allows a somewhat overqualification of incidents, in which the computer does not play any instrumental role at all. Some demystifying and relativation has to be done to bring the phenomenon back into real proportions, avoiding the sensationalism of the media.

Theft of microprocessors is not a computercrime, even if their capacity increase as a result of new technologies drastically modified their economic value. But even then, the magnitude of the information technology criminality should not be underscored.

Scarcely a day passes without any newspaper-clip on computer-crime or fraud. Television picks up the item and visualizes the "hacking" techniques. The difficulty, however, is to bring those individual findings into some global figures and clear indicators. This seems, especially in our countries, to be too delicate, if not impossible.
There is a sphere of reluctance and unwillingness in communication of incidents. Banks, insurance companies or any other potential victim are not easily communicative on losses occurred through computer interventions. Image-loss, indirect consequences such as the thrust of the customers or the competitive position, all push towards secrecy and discretion. The simple anonymous transfer of information for statistical purpose to official instances, even international ones, is objected to; the interference of judicial authorities is considered as "counter-productive" ?.
Most known cases come in the daylight through indiscretion, erroneous behaviour of the criminal himself or when insurance companies oblige the client to do so before refunding any loss. Besides, some countries are more communicative than others [3]. For sure one can state that figures are incomplete, that guesses be considered with care and that we only know the top of the ice-berg, whether that means 1% as to the FBI, or 15% as to the very experienced Stanford Research Institute.

Since a few years a considerable number of official bodies or professional circles are, showing interest in gathering valuable information. All of it should be read with a critical eye, since under- or overscoring is likely. Nevertheless, figures are impressive and worthwhile to be recalled: SRI mentions 100 million $/year in the U.S., the FBI makes two billion dollars out of it [4]. For Europe, an interesting estimate is the one of the *Association Internationale pour l'Etude de l'Assurance*, which comes up with six billion dollars loss for Europe in 1988. A U.K. survey by the *Local Government Audit Inspectorate* led in 1984 to 80% of 320 interviewed firms having been victim of a computerfraud [5], while for 1985 four major British banks budgeted £85 million against computer frauds [6]. The French CLUSIF reports a yearly amount of nearly 8 billion FF of Voluntaristic or accidental damages.

It is not the purpose of this paper to recall the spectacular and classical examples such as the Equity-funding [7] or Security Pacific Bank [8], or Memorial Sloan Kettering Cancer Institute [9], the French ISOVER Case [10] or the CLODO activities [11], or many other [12] but it may be important to recall that not all incidents are linked to economic interest as such, but may equally concern health, privacy, morality or state strategic survival.

If the total size of computer abuses is substantially high, though not full-proof, it has also been proven that these totals concern a limited number of victims. Concentrating the losses upon few leads to the conclusion that the average gain of such crime is a hundred times that of the average classical hold-up, while the average time for the "discovery of the discovered" seems to be counted in years, not in months [13].

To be added to this picture is the great potential of the transborder dimension of information technology, whereby the physical presence of the actors upon the foreign territory is no longer necessary. This internationalization of this criminality adds a new dimension to the task of society in reacting against this phenomenon.

As to the actors themselves, they seem roughly to fall into two major groups: on one hand the computer-freaks, the youngsters trying to hack systems for fun, competition, challenge; whizkids or wargamers, i.e. "short-pants criminality", not necessarily with a clear criminal intent; on the other hand, wilful criminality by hackers or employees within the system, often highly qualified and technically skilled, often acting from within, abusing the hi-tech and jargon oriented "state in the state" position of the EDP-sector.

In conclusion on the characteristics of the phenomenon one can say that computers, whether used for simple data storage or retrieval, word processing, business activities, banking, electronic fund transfer, electronic mail, health care, R & D, defence systems, ..., are vulnerable to attack by experts or freaks, young or old, acting from within or without the area of operation of the machine, with results to be estimated with a mutative scale difference, since time, space or volume have no longer a limitative effect.

As to the different possibilities for misuse, – even if they can probably be technically described in a uniformed way – writers have identified several areas of incidents, but fail to bring them back in a uniform classification [14]. This harmonization need is now attempted through the channel of international bodies [15].

Roughly seen a categorization can be brought down along the following lines:

manipulation of data: input of false data, alteration, erasure, deterioration and/or suppression of stored data or programs with fraudulent intent.

data espionage: unlawful collection or acquisition and/or use of data.

computer sabotage: leading to the destruction or disruption of soft- or hardware. Extensively this may include any hindering of the functioning not only of a computer but also of the telecommunication system. Today this includes the phenomenon of viruses and worms.

unauthorized access or interception of a computer and/or telecommunications system with infringement of security measures.

program piracy with the infringement of the exclusive right of the owner of a protected computer program with the intent to exploit commercially the program. The same can be said of a protected chip or microprocessor.

Even if differences of labeling may occur under various initiatives [16], the major phenomena are clearly covered by the above list. As will shown below, not all countries accept the criminalization of all of these acts and the conditions of applicability are even more diversified.

2 The Computer Threat

It would be erroneous to overscore as well as to underestimate the vulnerability of the computer society. It is clear that from the angle of victimology, three major targets groups can be detected.

2.1. the **individual** becomes the weakest link in the new information technology era, not only from a sociological and economic point of view (loss of job security through robotics, word processing, etc...), but equally from the angle of legal protection (privacy).

2.2. the **economic targets** are also rather interesting: banks, insurance companies, corporations of all nature become more and more vulnerable, especially where networks are more and more flourishing, telecommunications more and more used, but still hardly protected, and the cost effectiveness of certain protections not yet shown. Direct and indirect losses will be substantial and the defence of the law too much of an after-the-harm reparation.

2.3. the **sovereign state** itself, who faces a so-called erosion of sovereignty when noticing that many raw data can and will leave the country for economic decision-making abroad (e.g. with the multinationals), the state having no insight in the departure of raw data or return of information and loosing impact on economic or financial decisions taken outside its operating or influence zone and nevertheless having to cope with the possessors of data and/or information.

The key finally becomes not so much the technology itself. It is mainly instrumental to a far more important target which needs protection: the legal interest violated, whether the individual human life, the survival of an economic entity or the independence of the nation itself. The technology adds something, be it speed, massification of data or transfrontier communication. It emphasizes or amplifies, without necessary creating new forms of criminality. Thanks to it, information radically grew in importance and with it all the values attached to it, whether intangible or not. Much value has to go to the notion of *information related criminality* or even asset protection management, in which, besides information, image protection and physical securization become equally important. The massive presence of computers and other devices in the whole flow of information in our society at all levels (international, state, firm or individual) may ultimately lead to an infiltration into the totality of the legal field, the criminal, as well as the civil, administrative, economic or constitutional one. The call for full re-assessment of the whole of the law to make the legal system respond better to the problems of new information technology is real.

Looking into the legislation of mainly the industrialized nations, one notices that in various countries answers have been formulated or are in the process of being formulated [17]. Their responses differ both because of the underlying legal system and of their appraisal of what computer-crime means to them today as a threat. Even if in the more regulated field of privacy protection the reference frame exists with the OECD guidelines [18] and the Council of Europe Conven-

tion for the Protection of Individuals with regard to Automatic Processing of Personal Data [19], national laws may show diversified implementation norms or techniques [20]. One has the feeling that national – if not nationalistic – approaches prevail, taking the territorial – thus national – character of the criminal law as a starting point. So is the response to the threats of economic recession or sovereignty erosion.

While information criminality has an important transborder facet and data will be easily send and handled abroad, the need for a more global, uniform or harmonized approach is not always perceived or accepted. A first and maybe not optimal trend, therefore, is the *all too national instead of cooperative* response to the phenomenon.

The efforts of the Council of Europe in the criminal field, or of the EEC in such areas as micro-processor protection [21] or data vulnerability as such [22], should receive priority attention and national legislatures should adjust to them quickly.

3 Trendsetting in Fighting Computer-Related Criminality

Out of the above findings, one must conclude that a valid response to the phenomenon requires a holistic approach, of which the three layers would be:

1. the security issue is a threefold one: it requires technical answers, managerial/organizational ones and legal responses.
2. within the legal sphere, different branches of law have to intervene (criminal law, civil law, intellectual law, labor law, etc...)
3. within the subsets of the law the international cooperation or coordination is indispensable.

3.1. The issue of *information security* cannot be addressed by the law only. Even if criminal sanctions or damage allowance have besides their reparation effect, an educational and preventive effect, it nevertheless is also true that the intervention of legal mechanisms mostly occurs at moments when the harm is already done and the incident consumed. Prevention prevails over repression. To that effect, the tackling of this issue requires an integrated approach of technicians, economists, behaviorists, organizational managers and lawyers. The responsibility of computer firms is involved to the extent that they ought to voluntarily accept minimum security standards or at least make their clients aware of the vulnerable aspects of their computerization and require them to take sufficient starting security measures in relation to issues such as physical integrity of premises, access controls and authentication procedures, the possibility or necessity for back-ups and contingency planning.

would do with existing definitions, eventually going as far as some extensive interpretations. This attitude seems to be limited today to a few countries, which seemingly have not been affected by the phenomenon or, at least, in which no major court activity in computer-crime is noticeable [28].
It is our contention that few, if no industrialized country will be left over in this category, as all nations will be facing serious challenges to the existing laws and the pressure for concerted action a.o. in the European context is strengthening.

The other reaction is to realize that new measures are inevitable. Therein, one can distinguish those who prefer a low profile adaptation, i.e. the analysis of existing concepts, testing their applicability to computer-related situations and, if needed, to take this dimension into account. This can then be done through amending the actual provision [29]. Others wish to enact clearcut new incriminations either as a specific bill [30], or as new provision or even as a new chapter in the penal code [31]. It has to be noticed, at the same time, that many countries are in the process of reviewing the whole of their penal code, which is certainly an excellent opportunity to include at an appropriate place the necessary provisions relating to information technology crimes [32].

In conclusion it seems correct to state that a large majority of concerned countries, together with international organizations such as the OECD or the Council of Europe, are well aware of the necessity to act at legislative level, even though with variable intensity. As will be shown in the following analysis, many states have indeed already taken initiatives or are in the process of doing so.

4.2 The Analytical Survey

The analytical survey of existing laws, drafts, loopholes and problems is not an easy task. Like many other scholars, we have the benefit of the outstanding expertise of Dr. Ulrich Sieber, who together with Martine Briat, was responsible for the survey conducted under the auspices of the OECD's ICCP [33]. The present analysis rests inevitably upon the same material and cannot be considered as exhaustive as the leading publications referred to. As in the OECD we start from the classical five-fold categorization: manipulations, espionage and piracy, sabotage, unauthorized use and unauthorized access. For once, the reversed order will be used, each time reaching a higher degree of criminality. To take the unlawful access and use as a starting point may be justified through the fact of their not so obvious association with the "crime" notion, their rather high frequency and potential danger, while at first glance, they belong to the least protected expressions of the phenomenon.

Unauthorized Access of Computer- and Telecommunication Systems. Notions such as "computerhackers", "whizkids", computer-time theft are already familiar. As of today there is no general penalization of this activity. Some countries have a specific legislation [34]. Analogies may be drawn from articles incriminating the entrance into one's property with false or unlawfully obtained

keys or wiretapping of conversations over PTT installations. In the field of privacy protection an occasional provision may be found punishing unauthorized access [35]. In some countries wiretapping of computer communications is punishable (Canada 178-11 Criminal Code) (Belgium Telecom. Law 1930) (U.K. Interception of Communication Act 1985). The Swedish privacy act (1973) includes a provision applicable if no other incrimination can be applied. So does the German Second Law for the prevention of economic crime (1986).

Others, like the French provisions or U.S. proposals [36] go all the way towards the inclusion of such a provision. It must be stressed, however, that such provision should be – and mostly is – conditioned with several elements such as:

- a specific intent (knowingly, without color of right)
- the violation of security measures
- a special request by the victim.

Often criminal prosecution will be waived if the perpetrator informs the victim of the act and indicates the loopholes in the system.

Unauthorized Use of Computer- and Telecommunication Systems. Most countries do not provide a specific provision on unlawful use (furtum usus). Sometimes, one can rely upon unlawful use of somebody's property, which would more point to the hardware use. This would be possible under Danish, Finnish or English law. In other countries, concepts such as theft of electricity might be applicable (Belgium), while others require the abuse of specific objects, such as cars or bicycles (Netherlands, Germany). Considering this diversity and the rising number of incidents of this nature, the experts both at OECD and the Council of Europe opted for the introduction of specific provision in the minimum model system. Initiatives were already taken at individual levels. Canadian (Criminal Law Amendments Act 1985) and American (Counterfeit Access Device and Computer Fraud and Abuse Act 1984) initiatives have already come through, while the guidelines for national legislatures of the Council of Europe puts the unauthorized use in the so-called optional list.

In the light of this consensus trend, uniform requirements would be a preferable goal. Again one may include:

- specific intent
- infringement of security measures
- intent to cause harm or another form of computer-crime (loss, e.g.).

Such a provision on "furtum usus", if made specifically for information technology issues, requires a clear definition to distinguish between information-processors which should remain outside the scope (wrist watches, pocket calculators) and the real targets, while emphasis should go upon the functions performed and not upon the technological assets, since the latter will be subject to continuous evolution [37].

Finally, it has to be mentioned that such unauthorized use will often occur within the frame of an employment relationship or of a service contract. This indicates that much can be achieved through clear formulation of rights and duties in the contractual or organizational area, and also through security awareness initiatives in DP environment.

Computer-Sabotage. If one considers in this the destruction and/or damaging of computercenters, data or other items linked with the computer, it is clear that this concept goes beyond the physical "terrorism" against corporal elements, but also concerns intangibles such as the data or programs themselves. Phenomena such as viruses and worms resort under this concept. This latter part is mostly not covered by notions such as property damage, vandalism, malicious mischief, since information can e.g. be erased without damaging or destroying the physical carrier. Therefore, countries, in which specific computer-crime law exists or is in preparation, do foresee either a specific comprehensive provision on this issue (American state laws e.g.), or an adaption to the traditional concepts (e.g. the Canadian new sections in the criminal provision on "mischief": mischief in relation to data). Austria, France, Denmark, West Germany, etc..., seem to go for specific computer sabotage provisions, as does the Council of Europe. It clearly indicates that besides the classical protection of tangible property, in one way or another the introduction of penal protection against damage to data or programs is to be suggested. Again, we would plead for a rather high threshold, including:

- specific intent
- detailed description of acts (destruction; damaging, rendering useless, meaningless or ineffective)
- eventually, aggravating levels can be introduced if the target is an essential element in public administration or an economic enterprise.

Computer-Espionage. The major targets to be protected here are the computer-stored data, the special protection to be offered to computer programs and, recently the special protection of computer chips. If it is clear that the illegal appropriation of one's property is perceived as a crime and is covered by many existing provision such as theft, embezzlement, larceny, the specificity here relates to the fact that some of the targets are not of a physical nature, but constitute "intangibles", not covered by these provisions. A basic discussion related to this concerns the legal status of information.

If no proprietary rights are possible, can it then be subjects to "espionage" ? The protection of data stored in a computer system can eventually be looked upon from the *traditional property law angle*. The major problem of the intangible nature of information is sometimes explicitly solved by including express reference in the law (U.K. Theft Act 1968) (Australia) (USA) (Luxembourg

draft). Others rely upon notions such as extending the idea of theft of electric impulses, even though electricity is a tangible (hold a wire and you feel it), or assimilating because of the economic values involved (Dutch and Belgian case law). Fundamentally, we can follow the Canadian Sub-Committee on Computer Crime, when opting against the property approach. The reasons are to be found in the above-mentioned aspects, namely tangible property or intellectual public good; traditional property/intellectual property; theft of tangible/intangible. A specific provision is preferable. Other linkages can be found in the *trade secret and unfair competition* law, where many countries foresee criminal provisions within their trade secrets law (West Germany, Switzerland, Austria, Greece). Others only cover partial aspects (e.g. fabrication secrets in Belgium, France, Luxembourg) or rely mainly on civil damages remedies. For the US a recommended Uniform trade secret Act has been adopted by a series of states. The U.K., Canada and Australia have not many penal provisions available, but are in the process of elaborating appropriate responses. So are the Scandinavian countries. This trend deserves support. The balance to be found, however, is here also between the legitimate right of the "owner" or "developer" to have his economic values in data or programs protected and the right of society to have ideas and discoveries accessed by anyone. The transborder dimension of information transfer should add even more to the difficulty of phrasing appropriate provisions, while the specificity of some informations (military, privacy, hi-tech know-how) or of some "detainers" (government officials, police officers, doctors, ...) equally can lead to separate or special rules. Should there be a "informational secrecy" as extension of the classical "professional secret" ?

The way this provision should be foreseen can thus raise basic theoretical issues as to the status of the data which are intercepted. Anyway the interception or appropriation of data form part of a broader range of abuses, namely the attack against the integrity of computer- or telecommunication systems. This concerns more the right to undisturbed exchange of data than the consequences itself of acts of espionage.

It would, therefore, be interesting not to cover the data or programs as such, but to search for the penal protection of the integrity of computer access of it. As conditions could be foreseen: the intent to harm.

As to the additional protection of computer programs, leaving aside the unsolved problem of the intellectual property priority of copyright over patent law or/and a sui generis solution [38], the main trend towards the copyright provisions should be followed in a spirit of harmonization, together with a strengthening of the penal sanctions in them, as was done in Italy (law of 1981), Sweden (1982), Finland (1984), West Germany (Copyright Amendment Act 1985 or the U.K. (Copyright Amendment Act 1982).

Computer-Manipulations. This is considered as the modification of data to change the processing and/or the output in order to obtain a change in information or at the expected consequence. In the latter case, one is back into the

"property" issue, (fraud, e.g.) with all its difficulties; in the former, forgery is the major available notion. As to fraud, the deception of a computer to meet the requirement that a "person" be deceived, seems problematic. Breach of trust is either limited to qualified persons or also requires a physical transfer of specific objects. Forgery is based upon visually readable documents, humanly understandable. Solutions de lege lata seem indispensable and are already available or under way. New laws are to be found in Sweden (Swedish Data Act 1974), the U.S. (Credit Card Fraud Act 1984) (Counterfeit Access Device and Computer Fraud and Abuse Act 1981), Canada (Criminal Law Amendment Act 1985), Denmark (Data Kriminaliteit Law 1985), West Germany (Second Law for the Prevention of Economic Crime 1986). The Council of Europe expert report lists computer-related fraud and computer forgery among the "hard-core" offences to be covered by all member states [39]. Work is done in the Netherlands, Luxembourg and Belgium. Consensus thus seems reached as to the necessity to act in this sector. Requirements should be a special intent (to obtain an advantage, or to harm) and a formulation in terms of functions and not in terms of todays technology.

4.3 The Transborder Issues

One of the more likely aspects of the phenomenon is its transborder potential. The elaboration of networks, the development of international telecommunications and the presence of a "multi-nationals" oriented economy certainly affect the traditional patterns of information transfer.

This carries consequences to be located in the international criminal law sphere, more particularly those of the penal jurisdictional competencies and the cooperative mechanisms between sovereigns. Answers have to be found to questions such as the localization of the crimes, the territoriality or extra-territoriality of them, the character of the crime (immediate, continuous, collective, ...), the applicability of the cooperation structures (such as extradition, minor assistance, transfer of proceedings), the police-cooperation, the evidence issue when computer elements are included. Pluri-national incidents are likely to occur with the presence of things such as SWIFT networks, electronic mail, international airline reservation systems, etc...

As to the *competence-issue*, the theory of ubiquity may receive a new perspective, whereby the situs of the act, its instrumentality situs, the situs of the potential consequence and the one of the actual effective consequence are and difficult to locate and more diversified than the traditional "shot over the boarder" example.

Considering the non bis in idem principle, a clearer delimitation or at least classification of competencies could become indispensable. It again points to the necessity of harmonized legislations. This "international connectivity" throws new light upon concepts dating from the "before the computer" area.
In the cooperation issue, the problem of double criminality requires once more

a common approach. Elements of distant complicity or co-authorship require response. What also about the effect of certain additional measures imposed as a sanction, such as the interdictions to use data or programs collected or obtained in violation of criminal law provisions. How does the notion of rogatory commissions apply to evidence stored in a foreign database, having an intangible character or/and being accessible from front-ends in the requesting state. How is seizure and restitution of data conceivable between two states. Many are the questions raised, few are yet the answers. The work in the Council of Europe did not lead yet to some specific ones [40].

4.4 The Procedural Issues

As for the transborder situation, a number of problems may occur in the domestic sphere. The most important issue seems here to be the admissibility of computer records as evidence. Most continental law countries have given much power to the criminal judge in the free evaluation of introduced evidence. It could be that no problems arise, even though the problem of authenticity of the evidence may play. In the common law countries, computer evidence may be regarded as "hearsay evidence", basically inadmissible.
Exceptions are made or in the make, such as the U.K. Police and Criminal Evidence Act (Bill S-33). Requirements of accuracy, knowledge of the existence of the automated system and its proper use, complementary or to be supplemented by other proof may be retained.

5 Conclusion

The world of new information technology is one of the most evolutive ones. The somewhat mutative effect of certain of these inventions equally affects the legal components of societal adaptation to them. But law is not knowledgeable for quick responses and immediate flexibility. Especially criminal law should be preserved from an all too hasty reply to timely phenomena. There is a need for a minimum of stabilization of acts or attitudes felt as a danger to society, a sort of confirmation of the discovery of new anti-social behaviour and the clear creation of a sufficient consensus for penalization of it. The computer abuse area has now reached the confirmation phase: facts are clear, continuous and increasing in number and inventiveness. The telecommunications area is now part of the criminal scene, maybe not fully in the open because of the technical unawareness of the victims or their attitude of overdiscretion, but equally vulnerable. The time to respond is there, if we do not wish the phenomenon to grow unharmed, considering the loopholes in the law and the legal vacuum in the transborder aspects of it. Concerted action seems to be the only efficient one, either through conventional way or, at least, through the search for common thresholds. The work of the OECD and the Council of Europe should be regarded as the guiding

trends, allowing coherent law-making activity in national parliaments. The balance between overcriminalization and the actual status of underlegislation still has to be found in many countries. To build upon a broader perspective than the national frontiers and to benefit from international expertise in the field seem to be cornerstones for effectiveness. The challenge is real, the social duty to respond to it is also within the hands of the legal profession.

References

1. It seems that every major writer in the field handles its own terms. See:
   SCHJØLBERG, *"Computers and penal legislation"*, Oslo, 1983, p. 3;
   SOLARZ, *"Computer technology and computer crime"*, Stockholm, 1981, p. 23.
   The computer is sometimes the instrument or target of an act (VON ZUR MUHLEN, *"Computer Kriminalität"*, Berlin 1972, p. 17); The specific purpose (PARKER, D.B., *"Computer Abuse Assessment"*, Washington, 1975, p. 3); Bequai only goes for "part of larger forms of criminal activity: white collar crime" (BEQUAI, *Computer crime*, Lexington, 1978, p.1).
2. OECD-ICCP, *Computer related crime - analysis of legal policy*, Paris (1986), p. 7.
3. See U.K.: A. NORMAN, *"Computer Insecurity"*, London, 1983 and K. WONG & FARQUHAR, W., *"Computer related Fraud Casebook"*, BIS Applied Systems, Ltd., Manchester, March 1983, 106 p.
   See also: Australia's information at the Caulfield Institute of Technology, Computer-Abuse Research Bureaus (CIT-CARB); Japan, National Police Department, *"White paper on computer crime"*.
4. Within SRI, D. Parker's publications are the more important ones:
   D.B. PARKER, *"Crime by computer"*, New York, Charles Scribner's and Sons, 1976, 308 p.
   D.B. PARKER and S.B. NYCUM, *"Computer abuse"*, U.S. Department of Commerce, Springfield, NTIS, 1973, 131 p.
   D.B. PARKER, *"Computer Security Management"*, Prentice Hall, 1981, 308 p.
   D.B. PARKER, *"Fighting Computer Crime"*, New York, Charles Scribner's and Sons, 1983, 352 p.
   Drs. J.C. VON DIJK R.A., *"Computercriminaliteit"*, Ars Aequi Libri (ser. Strafrecht en criminologie, dl. 3), p. 203, 1984; Ph. JOST, "Les pillards d'ordinateur défient le FBI", VSD, 27 jan. 1983, p. 10.
5. Local government Audit Inspectorate – Department of the Environment, *Computer Fraud Survey Report*, Crown copyright, July 1981, 33 p.
6. Scottish Law Commission, Consultative Memorandum no. 68, *Computer Crime*, (March 1986), p. 1.
7. L.J. SEIDLER, F. ANDREWS and M.J. EPSTEIN: *"The Equity Funding Papers, the anatomy of a fraud"*, New York (J. Wiley and Sons, Inc., 1977).
8. "10.2 Million $ theft may yield profit for victim", EDCAPS, Jan. '79, p. 11-12, Aug. '79, p. 14-15.
9. Whiz-kids managed to establish a link with a private network of the General Telephone Electronic Telenet.
   S. HERTEN, "Computercriminaliteit: er is nog toekomst in de toekomst", *Hume*, 26 Jan. 1984, nr. 2264, p. 32.