

Chapter 4. Cryptocriminals, a public concern

Communications, not easy at the best of times in Pakistan, were, quite literally, bugged. I eventually got through from Islamabad to speak to Jamila in Peshawar on the phone, only to be cut off after just a few words. When I redialled, the phone had gone completely dead. I asked the advice of the English journalist whose phone it was.

'Oh,' he said, not at all surprised, 'I know what it is. You were speaking French. The man listening in wasn't able to understand, so he's cut the line off and gone to find a colleague who can. Give him a few minutes to do so and you'll get through with no trouble.'

I followed his advise and he was perfectly right.

(Nick Danziger, Danziger's Travels)

Cryptography has a wide range of applications. As it can satisfy many good, even essential, needs in the information society, so it can be put to less noble purposes in the crime society. This chapter deals with the nefarious uses of cryptography: it will define in which ways encryption hampers law enforcement.

For a good understanding of the law-enforcement problems, one must analyze the context in which investigation takes place. Therefore, I will sketch some developments in crime (4.1) as well as in substantive criminal and criminal-procedure law (4.2), concentrating on the developments that are particularly relevant to ICT-related investigation. Then, I will describe relevant investigation methods, concentrating on gathering information in transport (tapping and traffic analysis, 4.3) and in storage (e.g., search and seizure procedures, 4.4). This will define the place of today's crime and crime-fighting in society, which enables me to analyze just what problems cryptography poses to law-enforcement (4.5). I conclude with an assessment of the essence and scope of the crypto-problems for law enforcement (4.6).

Obviously, law enforcement and cryptocriminals are issues society at large faces all over the world. With an increase in international crime and with the advent of the information society, cryptocriminals will more and more become an international problem. However, international or multinational investigation and cooperation is yet in its infancy – investigation continues to be very much a domestic issue. Problems and procedures differ in each country, perhaps not in essence, but at least in emphasis. I will describe the Dutch situation, and provide occasional side-steps to other countries that can serve as indications of how those countries would deal with these problems. The analysis in this chapter will serve as a case study, which may be transposed to other countries' systems and cultures as appropriate.

4.1. The crime society

In the 1950s, crime was not a prime issue in the Netherlands. Ordinary crimes such as theft and robbery prevailed. Two decades later, society was confronted with hijackers, psychopaths, and terrorist groups. Still, crime was mainly restricted to small groups operating on their own.

Then, in the 1980s, the Netherlands discovered a new phenomenon: organized crime.¹ Criminal organizations and organized criminals seemed to threaten society in ways and on a scale beyond imagination. They were supposed to penetrate the legal realms of society, they seemed to gain incredible profits which they invested in legal activities, and they began to spy on the police rather than suffer to be spied upon.

At the same time, with the rise of the information society, computer crime became more pervasive. Hackers hacked their way into Pentagons, viruses spread like a disease, and computer fraud rose significantly.

Society's answer to these new types of crime was to intensify investigation and to try and find new ways to combat modern crime. 'Crime-fighting' and the 'war on drugs' became buzz words in policy documents, as the legislator called for adequate measures to react to organized and computer crime. Laying bare the communicative patterns of criminals appeared to be one of the best methods of investigation.

This section deals with the criminal part of present-day society. It starts with a description of the new, serious forms of crime confronting society: organized crime, business crime, computer crime, and other forms of serious crime. I use these categories mainly because one can distinguish between typical perpetrators of these crimes. How and when these categories of criminals use information and communication technologies is of particular relevance to the crypto problem. I will outline the information behavior and the use cryptography of these various categories.

4.1.1. Organized crime

*They plan the overthrow of something,
Maybe by bomb, or gun, or spoken word.
That something exists. It modifies the words
Of the conspirators
(Howard Nemerov, Portrait of three conspirators)*

One can speak of organized crime when there are groups of persons who

- are primarily focused on illegal financial gain,
- commit crimes systematically with serious consequences for society, and

¹ It is a misconception that criminal organizations only came into being in the past few decades. As far back as the 17th and 18th centuries, criminal groups roamed the country; they would fit most present definitions of a criminal organization. [Duyne] Still, the 1985 parliamentary memorandum *Society and crime* stated that the Netherlands had in the past largely remained free from organized crime [18995, nrs 1-2, 47].

- are able to relatively effectively shield these crimes, in particular through showing willingness to use physical violence or corruption [Traa, 25].²

Organized crime is to be distinguished from business crime (or somewhat broader: organizational crime), which indicates members of a legal organization (primarily businesses) participating in committing offenses, while the organization does not as such function as a criminal organization (see 4.1.2).³

Contrary to what the term suggests, criminal organizations are not always well-structured and hierarchical. Rather, they operate in network structures or worldwide webs. One could speak of 'disorganized crime' [Duyne, 6], since the behavior of the organization is not ruled by market or company rules, but rather by the need to keep its activities secret from the judiciary. One could also speak of *organizing* crime, to stress the dynamic, ever-changing character of the criminal groups [Duyne, 18]. Flexibility and international cooperation⁴ are notable characteristics.

Activities

Criminal organizations engage in a range of illegal activities. Most specialize in particular areas, but some organizations are active in diverse markets. Besides financial crimes, the core activity of criminal organizations is trade in forbidden goods and services – formerly prostitution, gambling, and arms, nowadays mainly drug trafficking. The gains in this area are so high that at least part of the gain has to be reinvested in the 'upper world' (the legal realms of society). Money laundering is therefore an activity which any criminal organization somehow has to take part in; some specialize in laundering profits for other criminal organizations. Thus, modern crime is much more intertwined with the legal economy.

Apart from the main area of drugs, new areas of crime include trafficking in waste material ('waste crime'), nuclear materials, arms, and people (women, refugees, illegal immigrants). These require more specialist knowledge or have smaller markets, and are served by more specialized criminal organizations.

Another area that forms a great potential for organized crime is the area of taxes and subsidies. Especially in the European Union, the economy is being regulated through a complex system of taxes and subsidies, leading to large 'price wedges' between the costs of manufacture and of sale. This creates opportunities for organized fraud schemes. [22838, nr 2, 2]

2 Interestingly, the FBI definition is quite similar, except for the final part: "Any group having some manner of formalized structure and whose primary objective is to obtain money through illegal activities. Such groups maintain their position through the use of violence or threats of violence, corrupt public officials, graft, or extortion, and generally have a significant impact on the people in their locales or region of the country." [Abadinsky, 3] The "significant impact on local people" is US-centric, being largely inspired by Italian-style mafia and South American-style drug cartels.

3 I disregard the academic debate over the definitions of organized crime and business crime. Although the two overlap significantly (in many cases, business crime verges on organized crime, and the two are often interdependent), for the purposes of this book, it is useful to distinguish between (purely) criminal organizations and business criminals (who operate largely within a lawful context).

4 A survey by the German Federal Criminal Bureau (*Bundeskriminalamt*) found 67.5 per cent of the criminal organizations to cooperate with different nationalities. [Duyne, 24]

Seriousness

The past few years have witnessed an enormous increase in political attention for the problem of organized crime. Reading the reports and statements of policy makers, one gets the impression that society is shaking to its foundations. The 1992 memorandum on organized crime in the Netherlands reads: “The threat to Dutch society emanating from present-day criminal organizations must in our opinion be taken very seriously, given the far-reaching economic and moral implications.” [22838, nr 2, 6] In discussing this memorandum, the Minister of Justice and the parliament were of the opinion that the seriousness of organized crime can hardly be overestimated [23047, nr 6, 3]. UN Secretary-General Boutros-Ghali, addressing a 1994 UN conference, warned against the destabilizing effects: “Transnational crime, however, undermines the very foundations of the international democratic order. Transnational crime poisons the business climate, corrupts political leaders and undermines human rights. It weakens the effectiveness and credibility of institutions and thus undermines democratic life.” [Boutros-Ghali]

The financial gains and turnover of organized crime cause significant losses to the economy, as well as serious damage to the environment. Moreover, the potential interweaving of criminals in the upper world could form a serious threat to the stability and integrity of the entire society – and to its functioning as a democratic constitutional state.⁵ However, there are no indications that organized crime has systematically infiltrated specific sectors or free professional groups, such as attorneys, notaries, or accountants [Traa, 50, 56].

Organized crime takes place in the dark recesses of society, and it is difficult to assess its real extent and threat. There is no method to assess the ‘how-badness’, and therefore one may easily create spooks [Duyne, 193].⁶ One *can* say, though, that there has been an increase in organized crime over the past few decades, to such an extent that organized crime is a significant part of today’s society. The potential threats to the economy and the integrity of our society are obvious, but it is difficult to estimate the scope of these threats.

Information behavior

Criminal organizations must communicate in order to plan and perform their activities. They have a high need for communication.⁷ As the organization is larger and its operating field is bigger – often covering several countries – the criminals must use telecommunications to discuss their plans, give orders, convey information on where and when to operate, and warn each other against pursuing police agents.

5 According to the Dutch criminologist Hoogenboom, society might suffer more damage in the future through the offenses committed by legal corporations, and sometimes also by administration, than by organized crime. [*Staatscourant* 4 April 1996]

6 One might wonder what caused the sudden government attention for organized crime. Schmid suggests three reasons: 1. The government needs a new enemy after the collapse of the Eastern bloc. 2. Ministries need more money, and so they create problems to combat. 3. There is really something amiss. After some consideration, Schmid opts for the third reason. [Schmid, 7]

7 “Organized crime is characterised by, among others, the fact that the criminal behavior is thoroughly planned and presupposes the cooperation of several perpetrators, who particularly in the planning phase have a large communication need.” [Thiesen, 49]. “Especially criminal organizations, with a view to executing their actions, often have to rely on intensive communication.” [23047, nr 3, 2]

In general, criminal organizations have enough money to use the newest technologies. The telephone has been used since its invention to commit crimes.⁸ Lately, facsimile machines, mobile communications, and computer networks have proved welcome additions to make communications easier and more flexible. With mobile data terminals, one can exchange any message around the world from any place within seconds.

Of course, criminals are aware that their communications are being monitored. Although this does not always keep them from using communication means which they know to be tappable, criminal organizations are sophisticated enough to take efforts to prevent the police from hearing them. They are aware of police activities and anticipate new investigative methods.⁹ Increasingly, criminal organizations are shielding themselves from police scrutiny [Traa, 28]. For instance, a criminal group that operated a drugs line on Morocco and ripped drug consignments from other criminal organizations “did all possible to keep the internal communications secret” [Traa, 36]. An effective criminal must be a good information manager.

Criminals exploit legal and technical gaps in the police’s monitoring capabilities. Today, for instance, the police has difficulty in tapping certain mobile phones and data communications. Consequently, criminal organizations regularly use mobile phones, often a large number of them at the same time, and they use prepaid or stolen phone cards, which makes it difficult for the police to trace the right number to tap. “Some leaders of a criminal organization had an entire battery of pocket or car telephones at their disposal. None of these were registered on their own name. Others let themselves be beeped, after which they held their conversations only in public phone booths.” [Duyne, 174]¹⁰

A good example of information behavior is the group of Henk R., which imported and exported soft and hard drugs and produced XTC. The organization used modern communications equipment, such as pagers, mobile and car phones, and facsimile machines. The organization feared that the police was listening in on them and therefore did not use home telephone connections. Henk R. made sure all his people were continuously reachable by mobile or car phones. Furthermore, Henk R. had an interest in a telecommunications company in Amsterdam. This enabled him and the members of his organization to change mobile or car phones or connection numbers at any moment. This happened regularly, in particular when a drug consignment had been confiscated or when members of the organization were held by the police. The group also had unregistered phones at their disposal. Besides, telephones were purchased with false papers, and phones were registered on names of people who were not involved in the organization or who were even completely ignorant. [Traa, 193-194]

8 “The period since the Second World War has seen a democratisation of the telephone and a consequent increase in the number of offences committed with its assistance.” [CoE 82, 5]

9 Cf. the Second World War, when the phone was a relatively unfamiliar medium. People had the idea that the occupying forces could eavesdrop on all phone calls, which led them to largely refrain from using the phone for communications. Interestingly, as most telephone exchanges had been automated, the possibility of phone tapping was rather limited. [Hogesteeger, 32-33]

10 “The members of the organization communicate among themselves almost exclusively through car phones that can only be tapped with difficulty. In their houses and offices, several mobile phones are available for that purpose.” [22838, nr 2, 4]

Another common way of trying to thwart telephone taps is talking in codes. Instead of talking about drugs or consignments, people will use codes and seemingly talk about everyday affairs. Thus, one can hear: "I'll come and sell 10,000 sheep." [Duyne, 174] Whether this really hampers investigation is to be seen, especially when such diverse things are being ordered as "batches of jackets, stuff, young piglets, pure earth, milk, rooms", when it appears possible to order half a cassette or half a movie, and when a request is made to bring a pair of scales [Traa, 254]. Such 'codes' are easily crackable.

Use of cryptography

Not many cases are known of criminal organizations using encrypted communications.

An example of the pre-automated era are the rumrunners shipping liquor to the dry US in the 1930s. Although they used increasingly complex codes, cryptanalysts cracked message after incriminating radio message, culminating in leading cryptanalyst Elizebeth Friedman's cracking of the Consolidated Exporters Corporation radio traffic. The prosecutor acknowledged her worth: "Mrs. Friedman was summoned as an expert witness to testify as to the meaning of certain intercepted radio code messages.... Without their translations, I do not believe that this very important case could have been won." [Kahn, 802ff]

As, currently, tapping mobile phones can be made difficult by easy measures (such as using prepaid cards or various unregistered SIM cards), there is not yet a real need for criminals to use cryptophones. A Dallas detective noted "that the big drug dealers were not encrypting phone calls. Instead, they were swapping phones (using cloned phones) to stay ahead of law enforcement." [Denning 97d] The use of codes, however translucent, may indicate, though, that technologically advanced criminals could start using cryptography as the modern equivalent of these codes.¹¹

Some cases indicate that criminal organizations do use encrypted data transmission. The Danish police has, to a limited extent, encountered encrypted data transmission among suspects [Thiesen, 49]. A German jurisdiction leader stated that "hot business such as arms and drug trade is not any more done by telephone, but is being settled in encrypted form on the worldwide data networks." [Der Spiegel, 25 March 1996] And a White House official claimed that "organized crime members are some of the most advanced users of computer systems and of strong encryption." [EPLR, 13 September 1996] The Cali cartel allegedly used sophisticated

11 On the other hand, criminals may also turn to other communications means: "The current practice shows that suspects aware of the danger of being monitored shift to other ways of communication rather than send encrypted messages." [E. Schmidt-Jortzig, quoted in Moeller]

encryption for their telephone conversations [Denning 97d]. However, even if they will use encryption among themselves, criminals will have to communicate with the upper world in the clear – the more the organization tries to enter the legal realm, the more plaintext communications they will have to make.¹²

In general, criminal organizations are much more dependent on data communications than on data storage. They do not need to keep records of their transactions, and they can quickly destroy most of the incriminating information they have on paper or disk. If they have to keep data stored, it is probable they will try to shield these data, and cryptography is a likely means of doing so. Almost all of the organized crime and terrorist cases listed by Denning and Baugh in their directory of cryptocriminals involve stored encrypted files, not encrypted communications; the Walsh report found the same [Walsh, 3.2.1]. For instance, the Japanese religious sect Aum Shinrikyo, which committed a gas assault on a Tokyo subway station in 1995, had encrypted some of its computer files with RSA; the authorities were able to decrypt the files after they found the key on a diskette [Denning 97d]. In another case, Dutch police captured a PC with an encrypted partition they were unable to decrypt at the time. There was enough other evidence to convict the organized crime member, and when the disk was eventually decrypted, it was found to be of little interest. [Denning 97d]

But overall, it seems few criminal organizations presently use cryptography. The Dallas detective investigating a national drug ring said that “in the ten years he had been working drug cases, this was the only time he had encountered encryption, and that he rarely even encountered computers. He noted that the Ecstasy dealers were into computers more than other types of drug dealers, most likely because they are younger and better educated. They are using the Internet for sales, but they are not encrypting electronic mail.” [Denning 97d]

4.1.2. Business crime

Business crime can be defined as offenses committed by organizations that mainly rely on legal activities for their income; business fraud is the main example of business crime. In contrast to organized crime, business crime takes place for a large part in the upper world. Organizations that perform legal activities can commit fraud or waste dumping, but they have to maintain a legal basis. Whereas criminal organizations can easily give up front stores and start new ones without hampering their main activities, legal organizations depend on the legality of their main activity. The types of business crime committed are mainly financial offenses, such as tax fraud, money laundering, bribery, and forgery.

Seriousness

Business crime may involve large sums of money, and the interweaving of legal institutions and crime poses a threat to the long-term credibility of the rule of law. Therefore, business crime is an important issue for criminal investigation. The increasing importance of financial investigation to curb money laundering and large-scale fraud underlines this.

12 The Australian Federal Police stated that “much valuable telecommunications interception evidence and intelligence comes from targets talking to people who are not part of a criminal activity and who would not use encryption (arranging hotel, shipping or airline bookings is one obvious example.)” [quoted in Orłowski]

Information behavior and use of cryptography

The main goal of corporations committing business crime is not to make as much money as illegally possible, but to assure the survival of the company. Consequently, the corporation needs to conform to legal rules, and keep accounts and suffer tax investigations. This means that their reliance on information storage is much greater than is the case with criminal organizations. In the case of tax fraud, which is often assisted by forgery, a double account may need to be kept,¹³ and the 'black account' will need to be hidden. Cryptography may be a useful tool for hiding these kinds of activities. In practice, investigators found that in business crime cases, if cryptography is used, it is generally ready-at-hand systems, such as those in WordPerfect or Lotus. "Encryption in these cases was used mainly to conceal financial, procurement, and other business records. It was generally broken." [Denning 97d]

Apart from crooked businesses, fraudulent employees will also be a target for investigation. Their fraud often concerns deceiving the business itself in order to make money. This usually involves forgery, not secret data to be hidden in double books or to be shielded by cryptography. Occasionally, their computers may contain encrypted diaries or fraud-enabling software. Fraudsters operating on an individual basis or with one associate, a study on VAT fraud concluded, "tended to take no, or less sophisticated measures to protect their operation from exposure." [Aronowitz, 99]

When it comes to communications, the perpetrators of business crime will usually use common means of communication, such as the phone or the company's e-mail system. They often are less prepared for being tapped, and they will not likely use cryptography on the phone – unless this be a common feature of the company's communications policy. E-mail will often be in the clear, unless the company's policy is to regularly encrypt outgoing mail. On intranets, however, such regular encryption is more common.

4.1.3. Computer crime

Computer crime refers to all punishable acts in which the computer plays a significant part (cf. 2.2.2). Thus, hacking is a form of computer crime, as it can not be perpetrated without a computer. Destroying a computer is generally not regarded as computer crime, unless it be a computer that contains the only copy of a nearly finished dissertation – in that case, the fact that it is a computer rather than a ping-pong ball being destroyed *is* significant.

This definition refers to intrinsically computer-related crime. As I treat the problems of (computer-related) cryptography for judicial investigation, I will use a broader definition: computer crime refers to all punishable activities of which the perpetration or investigation requires knowledge of computers. Thus, a fraud committed with a computer – which could equally well have been committed on paper – falls within this broader meaning of computer crime: the police must have knowledge of computers to be able to investigate this fraud.

The main forms of computer crime are: fraud, forgery, computer sabotage, software piracy, and hacking [OECD 86]. A more extensive list, compiled by the Council of Europe [CoE 90], includes:

13 For instance, in 1985, a municipal fish market implemented a 'Roundabout System' (*BuitenOm Systeem*) to keep the sales of 'gray' fish out of the regular records [Charbon, 34-35].

- unauthorized access
- unauthorized interception
- unauthorized use of a computer ('joycomputing')
- alteration of or damage to computer data or computer programs
- computer sabotage
- computer espionage
- unauthorized use or reproduction of a protected computer program ('software piracy')
- unauthorized reproduction of a topography ('chips piracy')
- computer forgery
- computer fraud.

The Internet facilitates new forms of bad deeds which do not fall under these headings, such as spamming or unfair competition by abusing HTML metatags.

Computer-related crimes differ from traditional crimes, in that they are generally quickly executable, invisible, automatically and endlessly repeatable, and borderless, and they potentially involve high damages. Thus, computer crime can be at the same time highly profitable and hard to trace, making it alluring for criminals and 'respectable people' alike. Computer crime for a large part takes place in business surroundings, as the main perpetrators of computer crime are regular employees (see 2.2.2).

Apart from computer-related crimes 'proper', a number of traditional offenses are committed with computers, and therefore fall within the scope of the wider definition: they require computer knowledge to investigate them. The main offenses at issue are fraud and 'information crimes': hate crimes (such as calumny or propagating racism) and child pornography. Increasingly, perpetrators of these crimes exploit the potential of computer networks. As with other types of computer crime, they are hard to track down, especially in an international context.

Seriousness

It is difficult to assess the incidence of computer crime. There is a high dark number of unreported and – perhaps – undetected incidents. It is estimated that only a few per cent of all computer-related offenses are reported. The reasons for this obscurity lie mainly in the invisibility of computer crime itself and in the unwillingness of many companies to report computer crime incidents. Enterprises fear loss of respect and customer trust if it is known that their information security is flawed. Besides, they often prefer to handle incidents internally rather than have the police obstruct the continuity of the corporate network by its investigation. Moreover, most companies would be unhappy if the prosecution details the information-security flaws as evidence in a public trial.

Despite the difficulty of estimating the incidence of computer crime, one can say something about its development. Over the past decade, computer crime has risen, and there are various reasons to estimate that it will rise significantly in the near future. As the information society is taking shape, more and more areas of society are being computerized, creating new opportunities for computer crime. Moreover, the present young generation is growing up with computers integrated into their education, upbringing, and leisure activities. They will be

familiar with computers to an extent only a small part of present-day society is.¹⁴ If the level of security gaps remains the same (see 2.2.2), a lot more potential malefactors will attack the all-pervasive computer systems.

In a study on the future of high-technology crime, traditional experts (with law-enforcement backgrounds) and non-traditional experts (hackers) were asked about their assessment of future computer crime. “Child pornography, property crimes, data manipulation, and the criminal use of cryptology are some key areas of importance identified by [the traditional experts]. (...) Both groups agree that the focus of new criminal activity will include attacks on computer systems and the use of computers to commit fraud and manipulate data. These activities are likely to come in the form of counterfeiting, financial fraud, and software piracy. Advancements in computer technology itself will assist in the commission of these types of crimes.” [Coutorie, 26]

Information behavior and use of cryptography

Most computer criminals have considerable knowledge of modern technologies, and so, they are likely to use cryptography to facilitate or hide their activities. Computer fraud will be hidden in encrypted files, virus makers will use encryption techniques to make their viruses more persistent and obscure – or to encrypt and extort¹⁵, and hackers will store their bounty in encrypted form. For instance, the Danish hacker ‘Macronite’ encrypted his hard disks just before being arrested; as he refused to surrender the key, the investigation was stuck [Harbou]. Hacker Kevin Poulson used multiple-DES to encrypt files documenting his feats. These were cracked; allegedly, it took a Department of Energy supercomputer several months. In several cases, pedophiles and child pornographers were found to have encrypted e-mail and files; often, the culprits used PGP, likely because they generally are educated, technically advanced, and experienced Internet users. [Denning 97d]

As computer crime is mainly committed by individuals rather than by groups (excepting, perhaps, computer fraud by businesses), communication is less important an issue. Consequently, computer criminals will less likely use cryptography to shield their communications (a notable exception is closed groups of people exchanging child porn electronically). However, they may often use data transport, for instance in hacking, and here they can use cryptography or anonymous remailers to hide their activities. Warez user communities, who share illegally copied or cracked software, often use cryptography to exchange passwords needed for downloading – a journalist investigating the practice encountered a high number of PGP keys, and noticed that almost all warez sites contained cracked crypto software [Computable, 10 January 1997].

4.1.4. Other types of serious crime

Other types of serious crime relevant to the crypto problem are serious forms of non-organized, ‘traditional’ crimes. One can think of terrorism, kidnaping, murder, and armed robbery.

14 “Our society is about to feel the impact of the first generation of children who have grown up using computers. The increasing sophistication of hackers suggests that computer crime will soar as members of this new generation are tempted to commit more serious offenses.” [Kenneth Rosenblatt, quoted in Coutorie]

15 Cryptoviruses encrypting critical files were used to extort at least nine businesses in London. [Denning 97d]

In these cases, preparation of the crime can involve communication between perpetrators, or storage of data relevant to the crime. Although less likely than with criminal organizations or computer criminals, offenders may use cryptography to hide their activities from investigation, as in the case of Aum Shinrikyo's gas attack on the Tokyo subway.

Petty crimes are not a real issue in the cryptography debate. Usually, investigative powers such as tapping can only be used in serious crimes punishable with several years of imprisonment. Moreover, the police will be less dependent on automated information in investigating petty offenses, as these usually do not involve information transport or storage.

4.2. Investigation

Investigation used to be defined as all examination intended to clear up a presumably committed offense and to prepare the possibility of imposing a related criminal sanction [Corstens, 237]. It includes fact-finding, as well as measures taken to assure that the potential sanction can be executed, such as seizure to confiscate property. In this understanding, investigation can only take place when there is probable cause that a particular offense has been committed.

However, because increasingly, the investigation of particularly organized crime takes place in the context of laying bare networks of criminal groups rather than in the context of specific offenses, a broader definition has been proposed by the Van Traa committee. Investigation is: collecting, registering, and processing data and information

- on the basis of a reasonable presumption that punishable acts will be committed that, given their nature or the organized context in which they are committed, are a serious infringement of the rule of law, or
- on the basis of at least clear indications that punishable acts have been committed in order to arrive at a criminal sanction. [Traa, 455]

Dutch criminal and criminal-procedure law have been significantly changed to meet developments in the field of crime, particularly of organized crime. Moreover, several organizational measures have changed the outlook of investigation practice, and the stages in which criminal investigation takes place have gradually shifted. This section deals with these developments, to outline the context in which the investigation of organized crime, business crime, and computer crime takes place.

4.2.1. Developments in criminal investigation

Roughly speaking, the developments in criminal investigation come down to increasing attention for the informational and financial behavior of criminal groups, and to a general broadening of investigative powers.

In *criminal law*, three major topics are relevant. First, the 'loot-targeted' approach has been significantly extended in 1993. To attack criminal organizations where it hurts them most (money and fast cars), a convict can be dispossessed of his illegally acquired gains. To enhance the feasibility of executing this sanction, the police can seize property, such as bars of gold or Ferrari's, in anticipation of a court decision. The law, commonly referred to as 'Strip 'em', has yet to prove its value in practice; often, the loot tends to be untraceable.

Second, certain preparatory activities were penalized in 1994: acts in preparation of serious crimes to be committed in conjunction with others. Potentially, the law has a very broad scope. For instance, in theory, a lawyer who corresponds with a notorious drug syndicate leader on tax issues might be accused of activities in preparation of the offense of participating in a criminal organization (art. 140 DCC). The effect is that, especially where organized crime is concerned, investigation can take place in a very early stage, even before the (presumed) criminal organization has committed any offenses.

The third topic is computer crime. In 1993, the Computer Crime Act (CCA) extended the Dutch Criminal Code with several computer-related offenses, the most important being hacking, manipulating or damaging data (including spreading viruses), forging credit cards, and committing fraud with telecommunications services (such as phone freaking). In 1998, a follow-up Computer Crime Act II was proposed, to deal with liability of service providers, unauthorized access of protected e-mail, the power to demand decryption, and some more or less cosmetic improvements of the wording of the CCA provisions.

In the area of *criminal-procedure law*, the police has gradually acquired more powers. Since the introduction of tapping telephone conversations in 1971, the developments in telecommunications have forced the legislature to broaden the scope of this power to the tapping of all telecommunications traffic. The Computer Crime Act, along with the penalization of computer-related offenses, introduced new measures in 1993 to enable the police to investigate computer crime (referred to as investigating in 'automated surroundings') (see 4.3 and 4.4). The draft Computer Crime Act II revises the wiretap conditions and introduces some guidelines for Internet investigation, notably to allow pseudo-purchases via the Internet of data (read: child porn).

Recognizing that ICT will be an essential part of everyday life in the information society, the Policy Advisory Group on Computer Crime has proposed that *digital investigation* (investigating punishable acts committed with the help of any kind of ICT) be incorporated into everyday police work. Its June 1996 report [Beleidsadviesgroep] recommends that the ICT knowledge of the basic police staff be enhanced through education, so that they will know how to act when they encounter ICT in the course of an investigation. They should be supported by the more specialist investigation knowledge of the computer-crime teams. International cooperation and the development of the Internet are among the urgent issues to be addressed.

The stress on investigating the financial behavior of suspects has led to the introduction of a specific type of investigation: the *criminal financial inquest*, aimed at determining the illegally acquired gains. Such an inquest will help the judge 'strip' the suspect. Moreover, banks and exchange offices are obliged to notify the police of large and unusual financial transactions. Increasingly, financial investigation is seen as an outstanding means for investigating organized crime.¹⁶ One can assume that financial investigation and digital investigation will be major tools for future criminal investigation.

16 "Financial investigation is an entire way of working. From all activities within a criminal organization, you bring out all activities in the financial field. You look via those financial lines, who actually belongs to the criminal group. In practice, it appears you get a good overview indeed of who is really involved." [G.J.C.M. Bakker, team leader customs investigation FIID, quoted in Traa, 280]

Another development has been a gradual broadening of the scope of investigational powers, not through legislation but through case law. Consequently, procedural safeguards for suspects have been somewhat reduced – what safeguards were introduced are mainly due to European Court case law. For instance, whereas evidence resulting from an unlawful tap can not be used in court, the Supreme Court has allowed such evidence to be used in a trial against a different suspect who only later had become known. [HR 14 April 1987]

As the courts perhaps slowly slacked the restrictions on coercive powers, the police perhaps did more than was technically allowed, arguing: “What is not explicitly forbidden is allowed.” New methods of investigation – unregulated in the Code of Criminal Procedure – were put into practice, such as ‘peeping operations’ (breaking into sheds and garages to see whether an official search might be useful), the placing of direction transmitters, infiltration, and ‘controlled delivery’ of drugs. Eventually, there were so many signs that some police teams were operating on the verge of illegality, that a major parliamentary inquest was held into criminal investigation by the Van Traa committee.

IRT-gate

It was a voyage of discovery, prosecutor Van der Veen felt, like Columbus. Bruinsma and, after his liquidation in 1991, his three (‘Delta’) heirs were top criminals that escaped traditional crime-fighting methods. To knock-out the number one criminal organization of the Netherlands, new ways of investigation had to be explored. So, the InterRegional Team (IRT) of North Holland and Utrecht introduced the ‘Delta method’: delivering soft drugs under the secret direction of the police. Thus, an informer facilitating these shipments could grow into a civil infiltrator and gradually climb higher in the criminal organization, as he gained the confidence of Bruinsma and his heirs that he was a trustworthy criminal.

By September 1993, the police considered directing the marketing of a trial shipment of 100 kilograms of cocaine, in order to provoke a megashipment of 5000 kilos of cocaine. Then, the police would strike, and catch the Delta bosses. It never came to that. The supervision of the IRT had been transferred to the Amsterdam authorities in July 1993. In September, Van Kastel became the new IRT leader, and by the end of October, he discovered that the IRT was involved in the innovative Delta method of controlled drug delivery, for which he did not want to bear responsibility.

From then on, things went fast. Van Kastel discussed the affair with the relevant Amsterdam authorities, who informed the responsible ministers, and they decided to stop the Delta method. A press release of 7 December 1993 announced that the IRT had been dissolved, apparently because the Amsterdam authorities considered it the only way to stop the method from continuing. Many who had worked hard to set up the IRT cried out loud, arguing in public that other causes (corruption?) must have been the real reason for the dissolution of the IRT. A controversy was born. Feuds ensued between the Amsterdam crime fighters and their interregional colleagues (or competitors), between proponents and opponents of the Delta method, and between prosecutors and lawyers who eagerly took advantage of the increasingly available amount of information on illegal investigation practices. The police had ‘directed’ at least 100 tons of soft drugs to be marketed, and besides, several secret and unsupervised investigation methods came to light, such as ‘peeping operations’ that explored the usefulness of an official search or that placed cameras and direction transmitters. The supervision of these measures turned out to be seriously flawed (perhaps partly because some policemen would go ‘prosecutor-shopping’ to find a prosecutor who would give them the freedom they desired). People spoke of a breakdown of investigation authority. The press eagerly published all sordid details of the affair, and it became apparent that something was really rotten in investigation practice at large.

By the end of 1994, a parliamentary inquest chaired by Maarten van Traa had to set things straight. Its task was to find out what had really happened, and to suggest adequate regulations for investigation methods and for effective supervision to keep investigation within its proper limits. The Van Traa committee did a thorough job and in early 1996 published its ten-volume report *Regarding investigation*. Their golden rule ‘No power without responsibility, and no responsibility without giving account’ prompted new legislation that would precisely define the contents and limits of investigation powers.

Meanwhile, long after the dissolution of the IRT, the Delta method lived on in North Holland and Utrecht. After all, one could not risk stopping the activities of the infiltrator all of a sudden – he had to be ‘reduced’ slowly...

[Source: 24072, nr 14, Chapter 7]

The Van Traa report concluded that in several ways, criminal investigation had gotten out of hand. The 'crisis in investigation' was to be addressed by a thorough rethinking and reordering of investigation, with legislation detailing which powers can be used in which circumstances. The recommendations and parliamentary discussions were followed by a reshuffling of police officials, clearer controls on investigation practices, and legislature proposals regulating investigation powers, in which a balance was sought to define investigation powers in enough detail to be clear without becoming a straight-jacket. The draft legislation targeted special investigation powers, police registries, and pledges to criminal witnesses.

Draft legislation

As of 1 July 1998, the Dutch legislature is considering several legislation proposals in criminal procedure law. The following are relevant to the crypto debate.

Special investigation powers

Resulting from the IRT-gate debate, the draft law on special investigation powers [25403, nrs 1-2] is a major proposal to redefine investigation powers and to introduce several new ones. It aims at laying down strict conditions under which the investigation powers can be used, and to check their use in practice by sufficient supervision measures. With the introduction of a new 'suspicion criterion' – the reasonable presumption that someone is involved in the scheming or committing of organized crimes – it extends the scope of investigation (which, so far, targets only specific crimes that have been committed) with cases that center on organized crime in general. Moreover, some of the investigation measures (such as infiltration and pseudo-purchase) can also be performed by civilians. The investigation measures dealt with in the draft are: observation, infiltration, pseudo-purchase and pseudo-provision of services, systematic information retrieval, 'recording' a private place (largely, a 'peeping operation'), 'direct eavesdropping', wiretapping, and gathering telecom traffic data. Having been introduced in June 1997, the proposal still awaited discussion in the Second Chamber as of July 1998.

Crown witnesses

Another result of IRT-gate is a draft law to regulate 'pledges to witnesses in criminal cases', which would allow the Public Prosecutor to bargain with criminals and give them some judiciary reward in return for their testimony in a serious case against another criminal. This crown-witness legislation was drafted in 1997 and sent to the Council of State for advice after approval by the Council of Ministers in April 1998. It is to be submitted to parliament by the end of 1998.

Telecommunications Act

To meet the effects of the liberalization of the telecommunications market, the Telecommunications Facilities Act is to be replaced by a Telecommunications Act [25533, nr 309]. It aims at strengthening the Netherlands' competitiveness, safeguarding the quality and accessibility of the telecom infrastructure, and protecting the public interests in accessing and using telecom facilities. Thus, it includes, for instance, provisions on liability, universal service, number policy, interconnection, and privacy. Also, it requires telecom providers to ensure that their networks and services are tappable from the start. Having been approved by the Second Chamber in April 1998, the proposal was scheduled to be approved by the First Chamber in late 1998.

Computer crime II

In some respects, the 1993 Computer Crime Act (CCA) is felt to be inadequate to deal with computer crime. An update law is being drafted, the Computer Crime Act II, which contains four major items: the liability of telecommunication providers, the power to read 'closed' electronic messages stored with a telecom provider for later distribution, the power to seize and confiscate data, and an extension of the power to demand people to decrypt. (Initially, the draft contained a provision to demand suspects to decrypt as well, but this was removed after protests from the legal community.) Besides, several textual improvements of the CCA provisions are proposed, and the terminology is adapted to the liberalization of the telecom market. The January 1998 draft had not been submitted to parliament by July 1998.

4.2.2. The organization of criminal investigation

In the Netherlands, the people involved in criminal investigation fall into three categories: the police,¹⁷ the public prosecutor, and the examining judge. Roughly, the public prosecutor leads the investigation process, while the police executes the investigation. In case of an inquest, the examining judge takes over the leadership of the investigation, in consultation with the public prosecutor.

The police, after a recent reorganization, operate in 25 regional forces and one national force, the National Police Services Force. The regional forces have the tasks of maintaining public order and giving help to the needful (under supervision of the regional mayors) and maintaining the rule of law (under supervision of the public prosecutor). In this last capacity, they investigate crimes.

The National Police Services Force consists of a great number of specific services. It includes the Central Criminal Intelligence Agency, which coordinates national and international investigation, and the Payment Traffic Detective Service, which coordinates and executes investigations into money and securities-traffic offenses.

With a view to combating organized crime, six special interregional teams (IRTs) were established in the early 1990s. They were each to investigate a special type of organized crime, such as heroin trade from Turkey or the production of synthetic drugs. Due to IRT-gate (see sidebar) and a lack of clarity regarding their position, their work has not yet fully budded.¹⁸ One national team with a similar task, the National Detective Team has been formed.

Similarly, in 1991, special teams were formed to investigate computer crime. The Computer Crime Teams conduct specific investigations and collect and analyze information on computer crime. They assist police teams with activities involving computers, such as searching a company with a large automated system, and examining seized computers. Their work is supplemented by the forensic computer-investigation division of the Forensic Laboratory, which aids in examining, among others, pagers, computers, computer files, and smart cards.

A number of specialist investigation services and teams perform additional investigative tasks. The most important ones are the Economic Surveillance Department, which investigates economic crimes such as illegal imports or stock-trade fraud, and the Fiscal Intelligence and Investigation Department, which investigates (serious) tax-fraud cases.

17 More precisely, law-enforcement agencies, such as police detective teams and special investigation services. I shall often refer to this collectivity as 'the police', using the common notion of police as 'crime fighters'.

18 Since IRT-gate, the teams are usually referred to as 'core teams', to not associate them with the past excesses of certain IRTs.

The special investigation services generally have a restricted task and limited powers in investigating crime. On the other hand, they have inspection competence. Thus, regardless of a suspicion of criminal activity, they can wield certain powers to check whether pertaining regulations are being complied with.

Of the other two parties in criminal investigation, the public prosecutor is closest to the police, leading the investigation. He decides to start an investigation, to start an inquest to be able to execute certain coercive powers, to close an investigation, and whether or not to start a prosecution. Once an inquest is opened, the supervision is referred to the examining judge, who can order coercive powers to be performed. In general, the execution of coercive powers, such as search, seizure, and phone tapping, lies with the examining judge, the public prosecutor, or police agents, depending on the gravity of the corresponding infringement of constitutional rights (the graver the breach, the higher the official needed to perform it), and on the urgency involved to perform the measure – in certain cases, lower officials can execute the coercive power if there is no time to wait for the higher official.

4.2.3. The stages of criminal investigation

The investigation process consists of several stages. The ‘pro-active’ stage is the stage when there is no indication yet that an offense has taken place. Once there is probable cause that a (specific) crime has been committed, the stage of investigation proper starts.¹⁹ When the public prosecutor wants to exercise certain powers, he can demand the examining judge to open an inquest. As soon as enough evidence has been gathered, the inquest is closed and a prosecution against the suspect is started. In this prosecution, the evidence gathered during the investigation is presented in court and examined by the judge.

The ‘pro-active’ stage was regularly not counted as belonging to investigation, but changes in the field have made it a significant part of investigating organized crime, where the focus of the investigation is on the criminal group rather than on a specific crime already committed, and where the investigation may also target the planning of crimes. The draft law on special investigation powers provides a basis to perform coercive powers when there is not a concrete suspicion of a specific crime. (Formerly, this was generally not possible,²⁰ as coercive powers require a warrant which can only be given in the stage of investigation proper or during an inquest.) The law does not speak of the ‘pro-active stage’, but refers to another ‘suspicion criterion’: investigation can also take place when there is a suspicion that serious crimes are being schemed or committed in an organized context (this is limited to crimes for which pre-trial detention is allowed or which form a serious breach of the rule of law) (proposed art. 132a DCCP).

During the inquest, grave coercive powers can be used, but the (impartial) judge allows them only if they are necessary for the investigation, taking into account the rights of the

19 One should bear in mind, though, that in practice, “in the investigation of organized crime, a distinction can hardly be made between investigation of offenses already committed and the investigation focused on laying bare criminal networks.” [23047, nr 6, 4]

20 The inspection powers of special investigation services can be used to gather information in this stage, but these powers may not be used primarily for investigation’s sake (which would be *détournement de pouvoir*, that is, abuse of power). If the special services find evidence of crimes while inspecting a case, they can proceed to investigate this (which, as continued application of their inspection power, is not *détournement*).

suspect and others whose constitutional rights may be infringed by the measures. Sometimes, the rights of the suspect can hamper the investigation. For example, a suspect's right to know that an investigation is taking place will render a telephone tap useless. A major revision has taken place of the inquest stage, in order to better anticipate such practical and legal problems. The drift of the change is to limit the inquest to investigation powers which directly require the personal involvement of the examining judge.²¹

At the trial, the information gathered during the investigation may serve as evidence. The only admissible sources of evidence are the observation of the judge during trial, statements of the suspect, of witnesses, and of experts during trial, and (written) records. The judge will use the evidence according to his personal conviction: he has a discretionary power to use evidence as he sees fit (as long as he complies with the minimum rules of evidence). According to the exclusionary rule, 'contaminated' evidence (resulting, for instance, from improper or unlawful investigation activities) will be laid aside. Sometimes, if the improper activities of the police have seriously breached the rights of the defendant, the judge can rule the public prosecutor to be dismissed in his prosecution. Also, the judge will need to be convinced of the truth and reliability of the evidence, and so, the police must act systematically and carefully when gathering evidence, following guidelines and accounting their acts. Particularly with computer-related evidence, special care must be taken to assure its integrity and authenticity.

4.3. Gathering data in transport

In the process of investigation, the police sometimes need to violate people's rights. For instance, in investigating the scene of a crime, they have to trespass into someone's home. Because of their gravity, infringements of constitutional rights require an explicit legal basis, and they have to be as restricted as possible. The ways in which the police can breach fundamental people's rights are called coercive powers. These can only be introduced through an Act of Parliament: the constitution requires that infringements of fundamental rights by law-enforcement agencies can only take place if they are embodied in national laws and if they are necessary in a democratic society for the sake of, among others, national security or the prevention of offenses.²²

The coercive powers that involve ICT-related information retrieval can be divided into powers that gather data in transport (4.3) and those that gather stored data (4.4). Gathering data in transport concerns retrieving the data *themselves*: tapping (4.3.1-4.3.2) and gathering information *about* the data: traffic analysis (4.3.3).

21 In the early 1990s, the Moons Committee proposed several changes in the rules governing the inquest. Some of these are being implemented in the draft law on the revision of the inquest [23251].

22 The European Court of Human Rights requires infringements of fundamental rights to be established by 'substantive' law, which may be an Act of Parliament or settled case law [*Kruslin, Huvig*].

4.3.1. Tapping

Telephone tapping is eavesdropping (monitoring or recording) public telecommunications as part of criminal proceedings or as part of national security [24679, nr 1, 4], or, broader, “clandestine interference with the telephone system in order to intercept a conversation.” [CoE 82, 5]

The power to tap phones was introduced in 1971, because “in the preparation and execution of the operations of criminal gangs, the telephone plays an important part.” [Lensing, 1011] Since then, it has become an increasingly popular means of gathering information, especially in the investigation of organized crime. It is not used so much as to gather evidence, but rather to get a clear view of the criminal organization concerned, so that the police can better and sooner intervene. Apparently, tapping is particularly useful where first offenders are concerned, or people in the periphery of a criminal organization, as they usually do not reckon with the possibility of being tapped [Reijne, 35-36].²³ Even with criminals aware of the danger of being tapped, the police will gain information on contacts and appointments.

Often, real-time interception is crucial, to prevent crimes or to act quickly on intercepted plans – notably to follow suspects or to intercept deliveries on the spot, and so to gain evidence. “Law enforcement agencies require a real-time, fulltime monitoring capability for the interception of telecommunications.” [96/C329/01]²⁴

Despite the costs, which can be prohibitive, the use of telephone taps has increased significantly over the past decades. The reasons for this are the rise in attention paid to organized crime, the apparent success in quickly gaining information on criminal organizations, the high density of phones, and an easing of judges’ willingness to give allowance.²⁵ Whereas in 1986, 1,088 taps were executed, by 1994, the number of taps had risen to 3,284 [Reijne, 19].²⁶ One should realize that one allowance of tapping may involve several connections being monitored, often for a longer period. Thus, one tap warrant can lead to over 80,000 conversations being heard.²⁷

Conditions

The legal conditions for applying a tap are as follows. The investigation must urgently require a tap (a consequence of art. 8 para. 2 ECHR). The case must involve a crime for which pre-trial detention is allowed (usually, an offense punishable with at least four years of

23 Another example of the use of a tap is the case of the ‘Exportteam’, where the phone of a civil infiltrator was tapped to see whether the information he gave was correct. [Traa, 272] Sometimes, to enhance the effectiveness of a tap, the police apparently consider leaking ‘disinformation’ to the press, to provoke suspects into discussing the ‘news’. [Traa, 287]

24 Likewise, the Walsh report concludes that “the availability of real-time decrypted communications is central to the investigative capability of law enforcement agencies” [Walsh, 1.1.9].

25 From interviews with four examining judges, it appeared that: “There is a clear increase. (...) The boundaries have shifted. (...) All in all, these things lead in certain views to a quicker application of [tapping].” [Breuil, 47-48]

26 The figures are inaccurate due to incomplete reports by the courts and, perhaps, differing definitions of what constitutes ‘a tap’.

27 In the Laundry case, which involved both the tapping of normal and car phones and of facsimile machines, 88,424 conversations were heard. [Traa, 226]

imprisonment).²⁸ The draft law on special investigation powers contains a revision of the tapping provisions. It includes a new power to tap in the not-so-called 'pro-active' stage, that is, when there is a suspicion that serious, organized crimes are being schemed (see 4.2.3).

Another condition is that there is a reasonable expectation that the suspect will participate in the conversation. Thus, not only suspects' phones can be tapped, but also, for instance, relatives' phones. This condition is somewhat peculiar, as in practice a large number of taps are so-called 'NN taps', being part of an inquest in which the suspect is not yet (formally) known. This allows a broader tapping of phones, since there is no suspect expected to talk over specific phones. In practice, NN taps can continue long past the moment at which the suspect really becomes known to facilitate this broader tapping, making the condition that the suspect should likely participate in the tapped conversations a parody rather than a safeguard. Moreover, it is sometimes useful to continue a tap even when the suspect has been taken into custody, and conversations from third parties (such as relatives) can also be important for ascertaining the truth. Therefore, the draft law on special investigation powers suggests dropping the condition.

If one of the participants to a conversation is someone who has a professional right of non-disclosure (mainly, lawyers, notaries, doctors, and clergy), the police can not monitor or record it (unless the professional himself is suspected).

Only the 'public infrastructure' may be tapped (home connections as well as mobile phones). Private networks (for example, a corporate or campus phone network) are beyond scrutiny. However, the forthcoming Telecommunications Act allows non-public networks and rented lines which are open to third parties to be tapped by decree; thus, intranets – say, a worldwide network of a multinational, consisting of rented lines – can be tapped. Wiretaps may also include in-house conversations overheard if the receiver has not been put down well [HR 21 March 1989].²⁹ Radio communications can readily be intercepted if this does not involve a 'special effort' on the part of the police. For intercepting radio communications that does involve a 'special effort', such as the use of advanced devices, or systematic and sustained interception, a warrant is required.

There is not a specific formal term for which the tap allowance can be given. Guidelines recommend a term of four weeks, to be extended each time with four weeks. The draft law on special investigation powers formalizes this term – one of the consequences of the *Kruslin* and *Huvig* verdicts of the European Court, in which the court judged that tapping must be "based on a 'law' that is particularly precise. It is essential to have clear, detailed rules on the

28 Tapping can not be used in the case of simple hacking, as traffic analysis will suffice (see below). In the case of 'onward hacking' (from one hacked site to another), the source from which the hack is perpetrated can not be recovered from traffic analysis, but this offense has been penalized with four years in order to allow content tapping.

29 Technically, the police could also listen in on conversations within a house even if the receiver is *on* the hook. By blowing up the capacitor of the phone with an electric surge over the phone line, the phone is automatically taken 'off hook'. This is still possible with many phones. Consequently, the police can claim that the in-house conversations thus recorded took place while the receiver was off the hook, and, referring to this court decision, use the recordings as evidence. According to Statewatch, the new UK telephone ISDN network uses a protocol with a built-in facility to take a phone 'off hook' and listen to conversations near the phone without the user being aware [Statewatch bulletin, March-April 1995].

The effectiveness of tapping

A 1996 study by the WODC (an academic, advisory center to the Ministry of Justice) investigated the practice and efficacy of tapping in the Netherlands. The study showed the following results on the effectiveness of tapping [Reijne, 35-44].

The goals of tapping – gathering evidence, tracking perpetrators, and uncovering criminal networks – are achieved in one half of the cases. Examining judges were of the opinion that in 70 per cent of the cases, the same results could absolutely not have been reached without a tap. Indeed, many interviewees indicated sometimes not to know how to fight organized crime without tapping. Examining judges particularly value tapping in cases of drugs, theft, and fraud.

With criminal organizations, tapping yields useful information on networks and financial gains. As the persons tend to be more wary of speaking overtly (considering the frequent use of codes), tapping does not often provide direct evidence. With business crime, however, evidence often results directly from facsimile tapping. On the other hand, some interviewees think tapping does not offer much for investigating business crime. With individual crimes, especially serious offenses against people, tapping generally provides direct evidence. Computer crime is not mentioned in the study. The study found that in 41 out of 91 cases, the tap did not yield any evidence. In 21 cases, the tap furnished direct evidence, in 15 cases, indirect evidence, and in 14 cases both.

One caveat in evaluating the effectiveness of tapping is the influence of interpreters, some of whom are considered unreliable; many interpreters select conversations without fully knowing the particulars of the case under investigation. It is also worth noting that the costs for interpreters have risen sharply, and now exceed the costs for tapping and printing [Reijne, 71].

The ultimate evaluation shows that two thirds of the interviewees consider tapping a reasonably to extremely effective means of investigation. Some, however, think the expectations of tapping too high, and consider tapping to often cost more than it yields.

A comparative study on wiretapping in Germany and the US is one of the few studies with figures on effectiveness in other countries [Böttger]. Based on the US wiretap reports of 1987-1989, the study found that in 95 per cent of the cases in which wiretaps were employed, incriminating conversations were recorded. Arrests were made in 47 per cent of the cases, whereas in 33 per cent of the cases, someone was convicted. In the cases in which at least one person was convicted, on average, another 8 to 15 persons were convicted as well, which the authors perceive as an indication that wiretaps are indeed efficacious in laying bare structures of criminal organizations. The figures suggest that wiretaps are less productive in yielding decisive evidence, since the incriminating conversations have not led to arrests or convictions in many cases. Or perhaps there are long-term effects the study could not incorporate. According to the 1997 yearly report of the Administrative Office of the US Courts, 20 per cent of all conversations intercepted in 1997 produced incriminating evidence (it does not say in which percentage of cases), leading to the arrest of 3,086 persons and the conviction of 542 persons, a conviction rate of 18 per cent of all persons arrested. The cumulative figures show that in 1997, the wiretaps completed in previous years led to 1,762 more arrests and to 2,352 more convictions. The number of convictions resulting from the 1988 intercepts, for example, increased from 543 in 1988 to 1,192 in 1989, and then decreased through 400 in 1990 to 57 in 1993 and 11 in 1996. [OA] The effects of wiretaps may therefore be slow but sure.

subject, especially as the technology available for use is continually becoming more sophisticated.”

Legal problems

One of the main legal problems with tapping is the requirement to notify a suspect that a criminal investigation is taking place against him. Naturally, once a suspect has been notified, the tap is useless. For this reason, the notification is usually postponed until the latest possible moment, just before the inquest is closed and when an indictment is near. The judges allow this postponement with a view to the efficacy of tapping. This point might also be an argument for public prosecutors to open an NN tap, even if they have enough reason to suspect someone in particular. The contradiction between the requirement of internal openness (the right of the defendant to know the activities of the prosecution) and the requirement of effective investigation has led the draft law on special investigation powers to

disconnect the telephone tap from the inquest. Tapping would also become possible in investigating the 'scheming of crimes'.

A related problem is the current requirement to destroy information and material that are no longer relevant to the investigation. Although intended to protect the suspect's privacy, the obligation leads to a situation in which the defendant can not check whether conversations have been transcribed (or translated) correctly, and he has no opportunity of demanding disculpatory information to be added to the file. Therefore, the draft law on special investigation powers requires the prosecutor to keep the original recordings until two months after the case has ended.

Technical problems

The rapid developments in the communications infrastructure are posing major challenges to the technical feasibility of wiretapping, through the introduction both of new networks and of new services.

New networks usually have different technologies, and so, tappability is not self-evident. For instance, ISDN seems difficult to tap. More importantly, the police has difficulty in tapping certain mobile phones. Although analogue car phones can be intercepted by scanning the spectrum,³⁰ with the advent of digital and satellite communications, tapping has become increasingly difficult. For instance, GSM uses encryption for the air interface, making scanning useless. Therefore, tapping GSM happens at the terrestrial infrastructure, which initially required considerable effort.³¹ Now, GSM and other digital mobile telephony, such as DCS-1800, are being tapped regularly. Satellite-based mobile phones are currently out of tapping's reach.³² The EU is working on a treaty to ensure interception capabilities of mobile satellite communications.

Still more problematic is tapping electronic messages. The main problem is the packet switching technology. As the messages are divided by, e.g., the TCP/IP protocol into many small packets, which are all routed over the network depending on the availability of capacity, it is virtually impossible to intercept all parts of a specific message along the way, unless the tap is placed close to the house connection of the sender or recipient. "This technology makes tapping complicated." [Dijk]

Like new networks, *new services* often rely on new technologies. Sometimes, these do not pose technical problems. Facsimile machines can be easily tapped, and this happens

30 This requires a judicial warrant, as scanning the spectrum and selecting the conversations of targeted suspects involves a special effort. In the case of Henk R. (see 4.1.1), the police listened in on Henk's car phones with mobile scanners; they had a warrant to eavesdrop for four weeks on all car phone conversations in which he participated. [Traa, 198] Pagers can be intercepted through scanning, like analogue mobile phones. Strangely enough, the Amsterdam court has considered the scanning of pagers to involve no special effort, so it would not require a court warrant. [Rb. Amsterdam, A.D.]

31 "GSM differs thus fundamentally in complexity from other services, and is estimated to be relatively difficult to monitor." [Nielsen, 37] According to the *Tapping GSM* regulation, GSM should have been tappable in the Netherlands by 1 January 1996 [24108, nr 5, 3], which was rather optimistic.

32 Satellite-based mobile digital telephones are "presenting prosecuting authorities throughout Europe with a problem. (...) [These are] seeking European co-operation in setting up a system to monitor international telephone calls made on this type of mobile phone." [Nash]

regularly.³³ For example, in the Tanker Cleaning Rotterdam case, phones and company facsimile machines were tapped for six weeks [Traa, 204].³⁴ Other services, however, make tapping more difficult, for instance because it is harder to find the right point to tap. Thus, a recent problem with intercepting mobile communications is the use of prepaid cards, which can prevent customer identification; this is one of the main problems today for tracing the user of a mobile phone.³⁵ Also, the *21 switch-based call-forwarding service has made wiretapping as such more difficult.³⁶ Likewise, calling houses which offer cheaper phone calls through international lines give criminals yet another opportunity of using more or less anonymous phones. The advent of Internet telephony adds considerably to the difficulty of tapping phones, because criminals can use this technology which, for the time being, is hard to tap. And the rise of mobile data terminals may make these things worse yet for the police.

A more general problem is the increasing variety of protocols and formats. Whereas formerly, only analogue conversations were transmitted over telephone lines, nowadays a telephone tap can also record digital signals. So, the police must first distinguish the communication protocol used, and subsequently identify the format in which the contents are transmitted (is it compressed digitized speech, a compressed image or video file, or perhaps a MIME-encoded WordStar text file?).

Finally, a technical problem is knowing which numbers to tap. With the liberalization of the telecoms market and the enormous growth in applications and services, people can have several telecommunication subscriptions with different providers (say, Internet access through XS4ALL over an ISDN line belonging to Telfort, a Libertel subscription for the telephone that uses the old telephone line belonging to KPN, and a mobile phone from Dutchtone). Thus, it is increasingly difficult to quickly have access to the subscriber information necessary to know where to tap. To address this, the government proposes to set up an information center which will collect the required data. [25533, nr 5, 133]

Maintaining tappability

With the implementation of the Computer Crime Act in 1993, all kinds of telecommunications can *legally* be tapped, including facsimile messages, electronic data transfers, mobile phones, and satellite communications. The *technical* feasibility of tapping all forms of telecommunications, however, is still dubious. Thus, as US FBI director Freeh stated: "Merely maintaining without expanding the ability of law enforcement to conduct court-ordered wiretaps is the single most important problem law enforcement faces today." [Freeh 95c]

33 Before 1993, the tap competence included only telephone *conversations* [HR 26 May 1992], and so, facsimile messages or data messages were not allowed to be tapped.

34 The fact that facsimile machines are regularly being tapped in China became apparent when a New Zealand tourist was expelled from the Tibet Autonomous Region. The Chinese authorities accused him of trying to subvert the government and split the country, because he had sent a facsimile message from the Lhasa Holiday Inn, in which he had mentioned having heard a bomb explode near his hotel. [TIN]

35 The government seems to hope that this may be redressed by technical solutions [25533, nr 8, 10-12], but this does not seem quite feasible. Registering the people that buy prepaid cards may ensure traceability, but this poses a significant privacy threat.

36 "With the currently available tap facilities, the judiciary can not listen in on conversations held through *21." [Dijk]

The authorities worry that this valuable investigation method is becoming powerless, and they want to assure its continued efficacy in the future. Thus, the Dutch government requires telecom providers through article 64a TFA to take the necessary technical measures to assure that their infrastructure is tappable. The cost for tappareability is theirs, while tapping is paid by the judiciary. The main action line of the government is to oblige all telecom operators to make sure their systems are fit for judicial taps from the start: "All public telecommunications networks and services (...) should be tappable from the moment of their introduction." [24679, nr 1, repeated in 25533, nr 3, 43] The draft Telecommunications Act, which is to replace the TFA shortly, incorporates this in article 13. In fact, it is internationally a common requirement: the EU and the US both require telecom providers to ensure tappareability of all forms of telecommunications.³⁷

The government may ardently wish to maintain tapping capability, but at the moment, tappareability is far from being the case when it comes to mobile phones and electronic data transfers. It will likely take several years before the police can tap all mobile phones, Internet telephony, and e-mail. The authorities are aware that – even with the guideline of mandatory tappareability – the potential for intercepting telecommunications may decrease, and they are looking for alternatives, such as direct eavesdropping.³⁸

4.3.2. Tapping in other countries

Although regulations and practices differ, almost all countries allow judicial taps. In the European Union, all countries have a legal regulation for law-enforcement tapping – Belgium was the last to introduce legislation, in 1991 (see [CoE 82] and [Huybrechts]). Moreover, like the 1995 EU Council resolution, the 1995 Council of Europe *Recommendation Concerning Problems of Criminal Procedure Law Connected with Information Technology* recommends states to impose obligations on network operators to "avail themselves of all necessary technical measures that enable the interception of telecom-munications by the investigating authorities." [CoE 95]

In *Germany*, the wiretap regulations have recently been adapted. The 1996 Telecommunications Act requires network providers to ensure technical tappareability (paying the costs themselves), and to provide yearly tapping statistics to the regulation authority. The Accompanying Law to the Telecommunications Act of December 1997 covers the personnel consequences of liberalization and aims at ensuring future tappareability by requiring all employees of telecom providers to cooperate in tapping. The Accompanying Law would also extend this cooperation requirement to operators of corporate networks [Wuermeling]. The number of taps has risen from 1,805 in 1987 to 3,499 in 1992 and 3,667 in 1995. [CR 1996 nr

37 The EU Council Resolution of 17 January 1995 calls "upon the Ministers responsible for telecommunications (...) to cooperate with the Ministers responsible for Justice and Home Affairs with the aim of implementing the Requirements in relation to network operators and service providers." The first requirement reads: "Law enforcement agencies require access to the entire telecommunications transmitted, or caused to be transmitted, to and from the number or other identifier of the target service used by the interception subject." [96/C329/01] For the United States, see 4.3.2.

38 "The present competence proposed [direct eavesdropping] can to a certain extent replace the decreasing possibilities to intercept telecommunications." [23047, nr 3, 2-3] See further 9.1.

Echelon

Even before the body of former Iranian prime minister Shahpour Bakhtiar had been found in Paris, his murderers were stopped by Swiss customs. On 7 August 1991, a day before the body was found, Teheran sent an (encrypted) message to its diplomatic missions in London, Paris, Bonn, and Geneva asking "Is Bakhtiar dead?" Then, French authorities monitored all communications from public phone booths on the Paris-Geneva highway, and intercepted a call from the perpetrators to the Iranian diplomatic mission in Geneva, essentially solving the murder before its discovery.

The interception of the Iranian communications was part of a US-led global surveillance system that has been operated since at least the early 1980s. Designed by the US National Security Agency, the ECHELON system regularly intercepts e-mail, fax, telex, and telephone communications around the world. The countries of the UKUSA signals intelligence agreement – the US, the UK, Canada, Australia, and New Zealand – operate an extensive network of stations that intercept the communications carried by Intelsat and other satellites, as well as those transported over land-based microwave networks. The intelligence agencies of the countries each scan the intercepts for key words, organized in a wide range of categories, that include names, addresses, and places of interests. (Although it may not yet be feasible to thus scan all spoken messages, high-volume voice-recognition technology may soon be capable of processing most telephone conversations as efficiently as written messages can be scanned nowadays.) Subsequently, with 'intelligent' agents based on statistical methods and neural networks, key words and their combinations are looked for to select the most interesting messages. These are forwarded to the headquarters, where specialists read them and act accordingly.

Despite earlier publications – as early as 1988, Duncan Campbell reported on ECHELON in the *New Statesman* – ECHELON only gained publicity in 1996 with the publication of extensive details by Nicky Hager, who had interviewed many New Zealand intelligence staff members. With the publication of a European Parliament document in early 1998, in which Hager's findings were repeated (along with a frightening number of other surveillance and control technologies), the global surveillance system seemed to receive wider attention by the institutions that safeguard democracy. So far, however, UKUSA governments seem to simply and happily continue global monitoring.

Although since the end of the Cold War, the global surveillance systems have often been justified by the need to fight terrorism and to facilitate economic intelligence, according to Nicky Hager, "by far, the main priorities of the intelligence alliance continue to be political and military intelligence to assist the larger allies to pursue their interests around the world. Anyone and anything the particular governments are concerned about can become a target." Thus, for instance, GCHQ, the UK intelligence agency, intercepted the communications of Amnesty International and Christian Aid.

Incidentally, one might expect ECHELON to suffer from large-scale encryption by governments, who in diplomacy and state secrets after all are well-known users of robust cryptography. Of course, the NSA had reckoned with that. A report by Wayne Madsen of 1998 revealed that for decades, the US government had routinely decrypted top-secret messages of 120 countries through a secret agreement with Swiss crypto producer Crypto AG. Their machines had been manipulated so that the secret key would be automatically and clandestinely transmitted with each message. The Iranian authorities, after the Bakhtiar killing, felt that their encryption scheme had been cracked, and they arrested Hans Buehler, Crypto AG's marketing representative in Teheran. He was questioned for five hours a day for nine months, but he apparently did not know the equipment was bugged. In 1994, two Iranians were convicted for Bakhtiar's murder, but the third, Zeynold Abedine Sarhadi, was acquitted. Madsen suggests one of the reasons may have been a tacit agreement to spare Sarhadi in order to avoid having to use the intercepted and decrypted communications as evidence.

[Sources: Hager, Madsen, Wright 98]

4, 256] There was a sharp increase in 1996, with 6,428 telephone connections and 1,911 mobile phone connections being tapped [DB].

In the *United Kingdom*, the power to tap evolved from the 17th-century power of government officials to intercept and open mail [Kahn, 172]. It was given an explicit basis only in 1985, with the Interception of Communications Act 1985 defining the conditions for law-enforcement, intelligence, and security wiretapping. Although it authorizes interception by warrant, it does not allow use of direct wiretap evidence in a criminal prosecution [LAB]. Still, during 1996 and 1997, "interception of communications played a part – often the crucial part – in operations by police and HM Customs which led to 1,200 arrests" [Roche]. The

wiretap figures (for Great Britain) have risen from 522 in 1989 to 1,047 in 1994 [Statewatch]; in 1997, there were 1,647 wiretaps [EPIC Alert 5.11].

In the *United States*, tapping is regarded as essential by law-enforcement agencies, but it is controversial with civil-liberties organizations. Part of the crypto debate has centered on the ability to tap at all rather than on regulating cryptography to maintain wiretappability. A Supreme Court decision (*Katz v. United States*) in 1967 that wiretaps were searches requiring warrants under the Fourth Amendment, led to the enactment of the Omnibus Crime Control and Safe Streets Act of 1968, which together with the Electronic Communications Privacy Act of 1986 today regulates the interception of telecommunications. The conditions for intercepting electronic communications (such as e-mail) are less stringent than for intercepting voice communications; the exclusionary rule (which rules out illegally acquired information as evidence) does not hold for electronic interceptions. [NRC, 84-86]

To meet the challenge of continued tapping capabilities, the 1994 Communications Assistance for Law Enforcement Act (CALEA) was enacted. This requires telecom providers to make their networks tappable. Especially the requirement to facilitate a maximum number of simultaneous taps has raised fierce discussions. After two earlier trials, the FBI published final wiretap capacity figures in March 1998, requiring the simultaneous tapping of over 57,000 lines nationwide [see FBI]. However, the CALEA deadline for meeting the tappable requirements, 28 October 1998, was considered unrealistic by the telecoms industry, especially since negotiations by industry and the FBI on technical wiretap

standards stranded, allegedly because the FBI insisted on far-reaching capabilities extending beyond CALEA. For instance, the FBI was seeking enhanced ability to track geographical locations of cell phones, and the ability to separate out content from signaling data of packet-based communications [EPIC Alert 4.15]. In mid-1998, the deadline for CALEA implementation was postponed until 30 June 2000.

In the US, the number of (both federal and state) taps has varied between 634 and 1,100 in the period 1984-1997. In 1997, 1,094 taps were placed. The majority of US interceptions involved drug investigations (73 per cent), followed by gambling and racketeering (both 8 per cent). [OA]

The efficacy of wiretapping is disputed in the US, as only few cases use intercepted communications as evidence. [Böttger, 12] The FBI, on the other hand, claims that “[c]ourt-ordered wiretapping is the single most effective investigative technique used by law enforcement to combat illegal drugs, terrorism, violent crime, espionage and organized crime.

The majority of wiretapping is conducted by state and local law enforcement. Last year there were 1,154 wiretap court orders nationwide for all of law enforcement but these court-ordered wiretaps are critical to saving lives and solving the very worst crimes suffered by the public. Moreover, that number is not expected to increase in any significant manner when the law already passed by Congress [CALEA] is fully implemented. (...) '[T]here is no intention to expand the number of wiretaps or the extent of wiretapping.''' [Freeh 95c]

In short, Germany, the UK, and the US have recently adapted their telecommunications regulations to ensure future tappability in the light of technical and regulatory developments. All have experienced a significant increase in wiretaps over recent years, comparable to the Netherlands. The figures show that wiretapping is used extensively in the Netherlands and in Germany (although less than in the Netherlands). The UK and the US are tapping relatively little.³⁹

4.3.3. Traffic analysis

Besides tapping phones to get at the content, the police can gain information from telecom operators about the communications as well. Not only can the content of conversations be useful for investigation, also the knowledge of who called whom when, how often, for how long, and from where is of interest. These traffic data can give a good indication of communications patterns and lay bare the structures of criminals participating in joint activities.

As traffic information is less privacy-sensitive than the contents of conversations, the competence to demand traffic data is less grave and, consequently, to be preferred to tapping if it suffices to gather the required information.

The public prosecutor and the examining judge have the competence to command people working with a public telecommunications operator to give information on conversations that have taken place, in which – presumably – the suspect participated (art. 125f DCCP). Although this suggests that the power can only be applied to *past* conversations, in practice, permission is usually given for requiring information on *future* conversations, so that the operator can take measures to be able to comply with this request. The application is only possible with offenses for which pre-trial detention is possible, as well as hacking⁴⁰; the draft law on special investigation powers would also allow traffic analysis when there is a suspicion that serious, organized crimes are being schemed. The conditions may be revised when the results of a study into the law-enforcement need for business data will be available.

39 There are several reasons why tapping is used less frequently in the US than in the Netherlands. For one thing, in the US, the judge supervises the application of wiretaps more closely, and he has to openly account for his considering the tap necessary. In the Netherlands, the examining judge authorizes the tap, but he does not need to openly motivate his decision. More importantly, the application of the subsidiarity principle differs. In the US, wiretapping is considered a last resort, more intrusive and graver than, for instance, undercover operations. In the Netherlands, wiretapping, although considered a grave measure, is found convenient in many more cases, and preferable over employing undercover agents. This difference may be partially due to a different conception of privacy. [Cf. 25403, nr 5]

40 Although only punishable with six months' imprisonment, hacking was added here, because traffic analysis is virtually the only way of tracing a hacker.

The digitization of telephone exchanges has enabled better and broader traffic analysis, as more data are stored automatically [23047, nr 6, 20]. Traffic analysis can be an important tool in investigation, although its usefulness must not be overestimated. It supplements the content scrutiny of tapping, but it can not serve as an alternative, because for many purposes, it is necessary to be aware of what is being said rather than that something is being said.

4.4. Data storage

The most common method of finding evidence is looking for it. One can of course first kindly ask people to hand over data (4.4.1), but if they refuse, the police can use graver measures. They can search for the information itself, and look for computers and data carriers for search and seizure (4.4.2); they can also use computers to search for data over a network (4.4.3). If the computer is access-protected, the police should be able to undo the protection (4.4.4).

4.4.1. Handing over data

As the competence to search and seize property is a grave measure, the police should first try other effective means to achieve the goal of evidence gathering (according to the principle of subsidiarity). Rather than seizing things by force, they can ask the keeper to hand over the (seizable) objects needed. The police should specify which objects should be handed over. The competence is limited when it comes to letters and people with a right not to give evidence because of their profession, and the command for handing over can not be given to a suspect.

As data are not ‘property’,⁴¹ the police need an additional power to command the handing over of data that may serve the investigation. This competence was introduced in 1993 with the Computer Crime Act. It authorizes the examining judge to command someone to hand over specific (automated) data relating to the crime or to the suspect. The suspect can not be given this command. The addressee can comply with the order by recording the data, bringing them to the court registry, or giving access to the examining judge (for instance, through an online connection). The way in which data are to be handed over is to be determined by the examining judge. In the case of encrypted files, this formulation, however vague, can not be supposed to include the

Criminal financial inquest

For the estimation of illegally acquired gains, a criminal financial inquest can be opened in order to allow certain measures; the offense concerned must be punishable with a fine of the fifth category (NLG 100,000). During the financial inquest, the examining judge can use the same powers as during an inquest. Thus, he can have phones tapped, request traffic information, investigate computers, and search and seize (this includes the power to search and seize letters and other writings, so it is likely he can investigate e-mail messages). For instance, in the Henk R. case, the financial inquest was focused on investigating the seized administration and tapping phones [Traa, 240]. The police has a general competence to command someone to give documents or data for inspection, although this command may not be given to the person who is the target of the investigation, and people with a right to non-disclosure can remain silent.

41 Despite two rulings by the district court of Arnhem, data are not considered ‘property’ in the sense of criminal law, as they are multiple and the product of mental rather than physical labor, and as copying them does not take them away out of someone’s power of disposal. Moreover, special laws address immaterial values, such as intellectual-property law.

competence to order that the data should be handed over in unencrypted form; this would imply that the keeper should first modify the data, and this is contrary to the intention of the article, which presupposes the integrity of the surrendered data.

Apart from the police which investigates crimes, special investigation services also have coercive powers. These services inspect compliance with special regulatory laws, such as tax or environment laws. Their competence differs from that of law enforcement. For instance, the Fiscal Intelligence and Investigation Department (FIID) can command people to show them relevant documents and files. The addressee has to comply with such a command, under penalty of six months' or – if denied wilfully – four years' imprisonment. The subject of an investigation provides the investigation agent with books, records, or other data-storage devices, or the contents thereof. The data must be provided clearly and without restriction, and copies can be made (art. 49 State Taxes Act). The wording of the article seems to imply that the data handed over must be in the clear, and so, decryption may be commanded.

4.4.2. Search and seizure

If necessary, the police can look for evidence contrary to people's will: with a search warrant, they can turn a house upside-down to recover pieces of evidence. These pieces can be photographed or otherwise recorded, or they can be seized to serve as evidence in court.

The ability to search and seize property includes the competence to search in computers and to copy data. After all, a house search is the gravest possible coercive power to dig up evidence. The *Cocaine in kitchen cupboard* case has interpreted it as a 'focused and systematic investigation,'⁴² in which closets may be opened (with force, if needs be), floors may be broken up, and clocks may be searched (taking into account the principles of subsidiarity (first try the least infringing measure) and proportionality (use as little force as is necessary)). Therefore, also computers can be subjected to a search. Analogously to the taking of finger prints, copies can be made of data stored in the computer. Thus, investigating stored data can regularly be executed. It can only be done during a house search, though, as looking in a computer to see if there is incriminating evidence can only be done through a 'systematic' investigation. Therefore, the police⁴³ can only look for electronic evidence in more serious cases – those for which pre-trial detention is possible (or in *in flagrante delicto* situations).

Another option for investigating computers is to seize them and subsequently investigate the seized object. This is a useful competence for stand-alones, laptops, diskettes, and personal digital assistants, which can be seized both in a search (e.g., when the police lacks the time to exhaustively investigate the computer on the spot) and while arresting or stopping someone, or in an *in flagrante delicto* situation. The seizure competence includes all objects that can serve to ascertain the truth or the illegally acquired gains. The search and seizure of letters or other writings is limited: there must be a clear connection with the offense or the

42 Such a 'focused and systematic investigation' can only be executed in case of a house search with a corresponding warrant; other ways of intruding in homes to look for evidence are restricted to 'casual' looking.

43 A house search should be executed by the examining judge, or, if his arrival can not be awaited, by the public prosecutor or, again in case of urgency, by an assistant prosecutor.

International investigation

As organized crime and computer crime take place in a largely international context, international cooperation in investigation is an increasingly important issue. Investigating criminal organizations operating in various countries requires legal assistance, notably for wiretapping and searching in other countries. Computer crime often involves online international investigation, for instance, because evidence is stored abroad or because the crime has effects in several countries.

International cooperation in investigation takes place on two levels. First, legal assistance is given by states based on a mutual agreement, usually a (bilateral or multilateral) treaty. Thus, foreign states can request the Netherlands to find evidence in a certain case. The examining judge can then use certain powers he has during an inquest, for instance, tap a phone or conduct a search. As the procedure for requesting legal assistance takes some time, this will often be inadequate to investigate computer crime. In 1995, the Council of Europe recommended adapting criminal-procedure laws to enhance the international investigation of computer crime. [CoE 95] For instance, the possibility to search online in computers abroad would greatly improve evidence-gathering in computer-related cases.

Second, joint investigation is called for in international cases. As many of today's criminal organizations operate internationally, state-bound investigation and the slow provision of legal assistance are insufficient. Joint investigation teams could serve the task of investigating organized cross-border crime. The EU Maastricht and Amsterdam Treaties call for closer police and judicial cooperation, including operational cooperation in investigating crimes. Such joint teams may be supported by members of Europol, the facilitating investigation service of the EU. The main task of Europol will be to assist member countries in investigation, mainly through facilitating information exchange, education, and research.

suspect, or the court must authorize it. For seizing letters entrusted to the postal or telegraph service, the examining judge can order the contents to be made known to the police, as far as they are apparently intended for the suspect or originate from him. There is hardly any case law yet to indicate whether this competence could be used to seize e-mail messages stored with a service provider.

Whereas special investigation services have more powers than the police to command information to be given, they have less powers to search for it if the subjects do not cooperate: they can not, e.g., as such conduct a house search or tap phones.⁴⁴ They can, however, seize property. Thus, the FIID can seize books, including computers and diskettes.

4.4.3. Searching elsewhere

While conducting a search in a computer, it is possible that the police find that data are not stored in the computer, but elsewhere in a network to which the computer is connected. If this other place of storage is beyond the limits of the search warrant – a likely case with networked computer systems, searching in the computer system elsewhere requires another warrant. Because requesting other warrants for the location where the other computer is located is both impractical and detrimental to the investigation (a suspect could easily destroy the information in the meantime), a specific power to search elsewhere in computers while conducting a search was introduced with the 1993 Computer Crime Act. The competence stops at the national border, as national sovereignty prohibits investigating in other countries (safe when specific treaties create a competence for cross-border investigation). Moreover, the power must involve data that are reasonably necessary for ascertaining the truth, and the computer systems located elsewhere must be legally accessible to the regular occupants of

⁴⁴ “In other words: according to general criminal proceedings, the suspect does not have to cooperate with the seizure, and the judiciary can look themselves; in special criminal proceedings, the judiciary may not look themselves, but the suspect must cooperate.” [Buruma, 218]

the location being searched. Again, letters and personal writings are protected analogously, so that probably e-mail messages stored elsewhere can not be read.

4.4.4. Providing access

Many computers are protected against unauthorized access. Therefore, the police will have difficulty searching a computer if they can not remove its protection. Article 125k paragraph 1 DCCP authorizes them, during a search, to request someone who is likely to know the means of protection to provide access to the computer, or to provide the knowledge of the protection. As the command can not be given to suspects, the police will have to address a system manager or, in case of a home personal computer, housemates.⁴⁵

With the introduction of the Computer Crime Act, it was already recognized that not only access to the computer could be protected, but also access to files – through encryption. Therefore, article 125k paragraph 2 DCCP was introduced, declaring article 125k paragraph 1 analogously applicable. Thus, the police can require someone likely to know the means of encryption (i.e, the key) to surrender the key or to decrypt. As usual, the suspect can not be addressed. I will further describe the potential and limitations of this competence in Chapter 8, when analyzing the option of commanding a suspect to decrypt. Note that usually the suspect is the only one with knowledge of the key, which makes the present competence virtually useless in practice. This is all the more so, because the police always copies the encrypted data for later investigation at the office – and then the power to demand decryption can no longer be given, the house search having ended. The draft Computer Crime Act II addresses this latter issue by allowing the command to be given when the search has ended, but leaves the former problem unaddressed.⁴⁶

4.5. Problems through encryption

Inevitably, cryptography will be used by criminals to hamper investigation. In this section, I will use the applications of cryptography detailed in section 3.2 to assess how criminal use of encryption may thwart the information-gathering powers of law enforcement. From this analysis, I will define the main problems to be handled in the second part of this book.

Encryption for the sake of integrity and authenticity will not hamper evidence-finding, as this leaves the original text in the clear.⁴⁷ Only encryption for confidentiality purposes renders the message unreadable. Also note that whereas cryptography hampers tapping, it does not obstruct traffic analysis. I will therefore restrict myself to confidentiality encryption hampering the retrieval of the contents of data.

45 Since family members to the third degree and spouses can remain silent, this will often be ineffective.

46 Initially, the draft proposal contained a provision to demand suspects to decrypt, under strict conditions. After protests from the legal community against this infringement of the privilege against self-incrimination, the provision was removed from the draft.

47 If, as is usual, a signed hash is used. If the entire message is encrypted with a private key, the police can use the public key to decrypt. Cf. 7.3.

4.5.1. Main crypto-problems

If *network providers* use encryption to secure their network, the communications transferred over their infrastructure will be out of reach of police tapping. However, the obligation for providers to assure the technical tappable of telecommunications infrastructure (art. 64a TFA; art. 13 draft Telecommunications Act) can be interpreted as prohibiting unconditional use of encryption by network providers. That is, if they use encryption as a standard feature of the telecommunications infrastructure, they should offer wiretapping officials the original signal as it entered their network. Naturally, providing the original signal will still leave the police empty-handed if the users encrypt themselves. Traffic analysis will in any case still be possible if network operators use encryption, as they are required to cooperate and to give these data to law-enforcement officers.

Encryption use by *service providers* will generally not hamper investigation. Telecommerce using encrypted (pay) services, such as video-on-demand, is not part of criminal organizations' communication patterns, and taps are not hampered by these.⁴⁸

The main problem for law enforcement will be encryption by *end users*. They will use encryption for securing both information transport and storage. As far as *transport* is concerned, financial transactions, teleworking, video conferencing, and other types of communications will increasingly be encrypted for confidentiality. Supposing that mobile phones and data communications can in the future regularly be tapped, criminal organizations and computer criminals, with their knowledge of computer technologies, are likely to shift to encryption in order to remain outside the reach of wiretaps. Then, encryption for escaping law enforcement will be used on a larger – or even large – scale. After all, robust encryption software and hardware is available around the world, sometimes even online and as freeware or shareware, such as the widely used PGP.

Moreover, as voice communications will increasingly be performed on digital networks, even across the Internet, encrypted conversations will be common. For Internet telephony, the program PGPfone is available from the Internet free of charge; it can be used for secure (voice) conversations on the Internet. Especially when encryption programs will be incorporated in general services, for example, in Internet protocols (IPv6), mail programs (Pegasus, Eudora), web browsers (Netscape Navigator, Internet Explorer), or operating systems (Linux, Windows), the use of cryptography will become common and all-pervasive. Then, also 'traditional' criminals, such as minor frauds, child pornographers, and individual serious criminals, will widely use encryption to thwart law enforcement.

So, cryptophones, cryptofaxes, and the encryption of e-mail, data transfers, and voice communications over digital networks make tapping ineffective: the clear text is only recoverable at both ends, and currently the police has no means to trace this.

In fact, encryption is only a threat to tapping if tapping is possible at all. Conceptually, tapping causes three potential problems. First, the signal must be intercepted and recorded, which is largely a physical and technical matter. For most of the communications, this is

48 The information on who is using which services will be interesting to law enforcement, as this can assist the making of perpetrator profiles. The present powers to request information or, if the service provider will not cooperate, to search and seize the provider's administration – including the power to request decryption (art. 125k para. 2 DCCP) – are probably sufficient for getting this information.

possible, although it may be difficult with the Internet packet-switching protocol to intercept all packets. Then, the signal must be interpreted, which is a logical problem: what do the bits and bytes signify, what kind of information is it, and what format is it in. Third, once this is done, only then does encryption come into view. If the file is interpretable as a certain type of file, the text, image, or sound may turn out to be encrypted. Supposing that the first two stages can be addressed through technological sophistication, encryption may gradually turn out to be the main problem for wiretapping. Encryption of data transport, then, is likely to be one of the main future problems for law enforcement, hampering the tracing of perpetrators, the uncovering of networks of criminal organizations, evidence-gathering in fraud cases, and, to a lesser extent, catching computer criminals. FBI director Freeh, in a speech meant to incite the US Congress to restrict encryption, stated that “drug cartels are buying sophisticated communications equipment. Unless the issue of encryption is resolved soon, criminal conversations over the telephone and other communications devices will become indecipherable for law enforcement. This, as much as any issue, jeopardizes the public safety and national security of this country. Drug cartels, terrorists, and kidnapers will use telephones and other communications media with impunity knowing that their conversations are immune from our most valued investigative technique.” [Freeh 95a] One should bear in mind, though, that such statements are aimed at convincing others of the necessity of restricting cryptography, and may not be unbiased. Privacy advocates often point out that “the FBI has not been able to point to a single case to date where encryption has hampered their investigation of a case.” [Hoffman 94] But then again, that may be because the police wants to let sleeping dogs lie.

Likewise, the use of cryptography for securing information *storage* (for instance, of accounts, e-mail folders, and villainous plans) is a threat to law enforcement’s ability to investigate. The current search and seizure procedures are widely inadequate to cope with encrypted files. Only in a small number of cases can the police require the decryption of enciphered data, namely, during a search when a non-suspect person knows the means of encryption (which will rarely be the case), and when tax officials require to see the books. Even then, faced with a demand to decrypt, the addressee might use a duress code to thwart the demand: he will produce innocent data rather than the original incriminating plaintext. Thus, the use of encryption for securing data storage is another main problem for law enforcement, especially relevant in investigating organized crime (think, for instance, of laptop computers or personal digital assistants containing address lists), organizational and business crime (especially if the books are encrypted), and computer-related crime.

4.5.2. Cryptocriminals in practice

There is little reliable information on cases in which cryptography has hampered investigations in practice. Most policy documents and statements by police officials confine themselves to stating the potential (imagined?) gravity of the problem and giving one or two notorious examples. The only extensive (public-domain) study of cryptocriminals was undertaken by Dorothy Denning and William Baugh in 1997. A world-wide query to submit cases of cryptocriminals resulted in a list of examples of terrorism, organized-crime, espionage, and child-pornography cases involving cryptography. Their findings suggest “that the total number of criminal cases involving encryption world-wide is at least 500, with an

annual growth rate of 50-100%.” [Denning 97a] In a considerable part of these cases, the police were able to retrieve the information, or they were able to convict the criminals regardless of the encrypted data. FBI director Freeh claimed that the FBI has seen the number of cases involving encryption or password protection increase from 2 to 7 per cent. [Freeh 98] In 1996, a bill was adopted by US Congress, the NII Protection Act, which requires the Sentencing Commission to report annually on the use of computer encryption to facilitate or conceal criminal activity, and so more definite figures for the US may be available in the future.

Some examples of cryptocriminals, apart from those already mentioned in section 4.1, are the terrorist group responsible for bombing the World Trade Center in 1994 and a Manila Air airliner in 1995. The laptop of member Ramsey Yousef contained encrypted files on further plans, which were successfully decrypted; however, much of the information was also available in unencrypted documents, and decryption was not essential to prevent the planned attacks. [Denning 97d] A gambling enterprise operating multiple sites linked by a computer system encrypted four years of accounts; the codeword was cracked by exploiting weaknesses in the crypto system, resulting in a plea of guilty. [Denning 97d] The police in Sacramento, California, found a number of large encrypted files with a person suspected of involvement in child pornography. The suspect refused to surrender the key. [Wayner 93] At a 1996 OECD meeting discussing crypto policies, “the Italian representative said he was unaware of any criminal probes defeated by use of encryption, but he reported that the Mafia was thought to be seeking access to strong U.S. encryption for its communications. This led Austria to ask whether anyone knew of cases of crooks using encryption. Denmark reported one case. Holland reported a case of suspected terrorists using high-grade encryption; when pressed for information about how the case turned out, the Dutch representative simply said, ‘The encryption gave us a lot of trouble.’” [Baker 96] One of the five computer crime teams in the Netherlands encountered encryption in about ten cases, involving, for example, hacking, money laundering, and drugs; in one of the cases, the encryption obstructed the investigation beyond repair [Komen].

4.5.3. Cracking evidence

So, that twenty-first century kid, that fast-track Infobahni, that arriviste crooning I-did-it-I-way, proved to be not only a scheming usurper, but a moron – who thought himself uncatchable, and therefore got caught with laughable ease.
(Salman Rushdie, *The Moor’s Last Sigh*)

If the police encounter encrypted data, what are their chances of decrypting? Where encrypted *communications* are concerned, the chances are slim indeed. If the police can record and distinguish an entire encrypted communication at all (which is not always easy, as they should know just where the communication begins and where it ends; or, with digital networks, they must select all packets of the message), they will likely not be able to cryptanalyze it. They only have a chance if they know how the communication is encrypted, and if the crypto system is weak enough to allow a brute-force attack. If the data are compressed before encryption, a brute-force attack becomes very difficult even with weak systems. Also, given the high number of conversations recorded in a single wiretap, many messages would have to be cryptanalyzed (remark that selecting relevant messages is

impossible). Perhaps most importantly, cracking communications through a brute-force attack cannot be done real-time; it will usually require at least several days and often weeks or months. This significantly limits the efficacy of the wiretap (cf. 4.3.1); and then, the police may be reluctant to use decrypted intercepts in court, as this will give criminals insight into their cryptanalytic skills and capacity – it could “provide a tutorial to criminal elements bent on eluding law enforcement” [US].

There are much better chances with *stored* encrypted files (cf. 3.1.4-3.1.5). It is easier to see or guess with which system the file has been encrypted (for instance, because the encryption program is stored on the same computer, or because a Crypto User Handbook features on the bookshelf), and so, a cryptanalytic attack can be better focused and more efficient. In practice, some criminals use easy-to-crack crypto systems provided with general software packages, and only the more technologically advanced use strong crypto systems such as PGP. More importantly, many criminals use weak passwords or passphrases, which can be fairly easily guessed with automated password-guessing programs, such as PGPCrack. Sometimes, the key may simply be found stored on a diskette, as the police found in the Aum Shinrikyo case [Denning 97d]. Since the time pressure is smaller than with wiretaps (the search alerts the suspects that an investigation is taking place anyway), and the number of encrypted files may be limited, a brute-force attack may be a good last resort if the stakes are high enough. (Indeed, the police could perform distributed attacks (see sidebar in 3.1.5) to use the idle computer power of all police offices, for instance with a screen saver program, to crack the most important files.)

That there is a reasonable chance of success is indicated by the fact that data recovery is often used by businesses who need to decrypt files encrypted by disgruntled or careless employees. Specialist companies provide such data-recovery services. For example, the US company AccessData “specializes in data recovery and decrypting information utilizing brute force as well as ‘smarter’ attacks. Regular clients include the FBI and other law enforcement agencies as well as corporations.” [Ad Hoc]⁴⁹ AccessData took twelve hours to crack the custom-encrypted files in a Bolivian terrorism case; AccessData software⁵⁰ also enabled the decryption of encrypted files in the Aldrich Ames spy case [Denning 97d]. Another possibility is that the manufacturer of the hardware or software has a master key.⁵¹ This way, the police may recover a certain part of stored encrypted files.

Indeed, the Denning-Baugh survey found that in organized-crime and business-crime cases, the encryption of stored data was generally broken [Denning 97d].

49 “AccessData (...) reports receiving about a dozen and a half calls a day from companies with inaccessible data. About one-half dozen of these calls result from disgruntled employees (...) another half-dozen result from employees who died or (...) forgot to leave their keys.” [Denning 96]

50 Phil Zimmermann reported a conversation with the author of the AccessData package that cracks many built-in encryption schemes in general products: “he said his program only takes a split second to crack them, but he put in some delay loops to slow it down so it doesn’t look so easy to the customer.” [Zimmermann 94, 105]

51 Cf. [HR 29 March 1994], in which the Japanese manufacturer of a pocket computer recovered the data from the protected secret memory.

4.5.4. Further crypto-problems

An additional problem is caused by the possibility of hiding encryption.⁵² The use of steganography to communicate without anyone noticing the exchange of information, e.g., through posting a message in a digital image to a news group, can be called the ultimate way to prevent the police from investigating communications patterns. Although impractical in cases of urgency or when two-way feedback is needed, it is a viable option for exchanging shorter messages when there is no urgency.

More damaging to law enforcement will be the use of steganography to hide information in computers.⁵³ Files can be stored hidden in images or sounds. The police may search the computer's contents, but may easily overlook the incriminating evidence. Indeed, to really hide incriminating files, smart criminals may even "concoct some mildly incriminating dummy messages to take the place of the really incriminating real messages. A pair of Israeli spies once did this." [Schneier, 228] One should not overestimate the possibilities of steganography, though. In many cases, the pattern of the image, sound, or text file will show that it is not an ordinary file. Moreover, there is bound to be some header information for the stegano program to be able to recognize the file as containing a stealth message.

Problems in proof

Apart from potential crypto problems for evidence gathering, cryptography may also cause problems in court. As computer-related evidence may result from highly technical procedures, a smart lawyer can cast doubt on the reliability of the evidence. A judge without a degree in maths will find cryptology abracadabra, and so, he will have to rely on the statements of experts.

Suppose the prosecution uses evidence resulting from encrypted information, obtained through either cryptanalysis or through decryption with the proper key (found somewhere or given by someone). The police will have to prove that the resulting clear text is indeed the original plaintext. The defending attorney may try to discredit this, saying there is no mathematical certainty that the given text is the right plaintext. However, as it is virtually impossible that a given ciphertext decrypts to two meaningful plaintexts, an expert witness will likely convince the judge of the reliability of the cryptanalysis or decryption. (Compare the *packet computer* decision, where the appeal court stated: "The proposition, that in Japan the secret memories of the pagers may have been tampered with, has not become plausible. The expert heard in appeal Professor Kaspersen did state that manipulation was not entirely to be excluded, but he added that he considered this a purely theoretical possibility. There is nothing that indicated this possibility." This statement was not challenged in cassation.) The judge must be convinced, however, that the police (or the Forensic Laboratory) has acted properly in obtaining the plaintext: after all, they might have XOR-ed the ciphertext with a conveniently incriminating plaintext to obtain a One-Time Pad key which yields – behold! – the incriminating, but false, plaintext. So, in the process of cryptanalysis or decryption with an obtained key, the police must act carefully and systematically, and must make official reports of all activities to ensure that the process can be checked by neutral experts. The defense might claim a right to a counter-check [cf. *Buruma*, 228-237]. It would be wise to have standard procedures for handling encrypted data, comparable to, for instance, the initial proposal for direct eavesdropping, which contained a prescription for the (automated) recording of each step in the process of treating the recordings to enhance their clarity. A similar procedure should be developed for cryptanalysis and, in general, the handling of encrypted evidence.

Perhaps the biggest challenge will be to find expert witnesses who can clearly explain to the judge how encryption and cryptanalysis work. The gap between the legal and mathematical jargons (not to say: world views) looms so big, that a judge might be hard to convince that this magic really works.

52 Cf. section 7.3 on stealth messages in digital signatures.

53 Although the presence of stegano-software would indicate that there are files hidden somewhere. A search on the images with a dictionary attack might render incriminating plaintexts (compare Illustration 4.1).

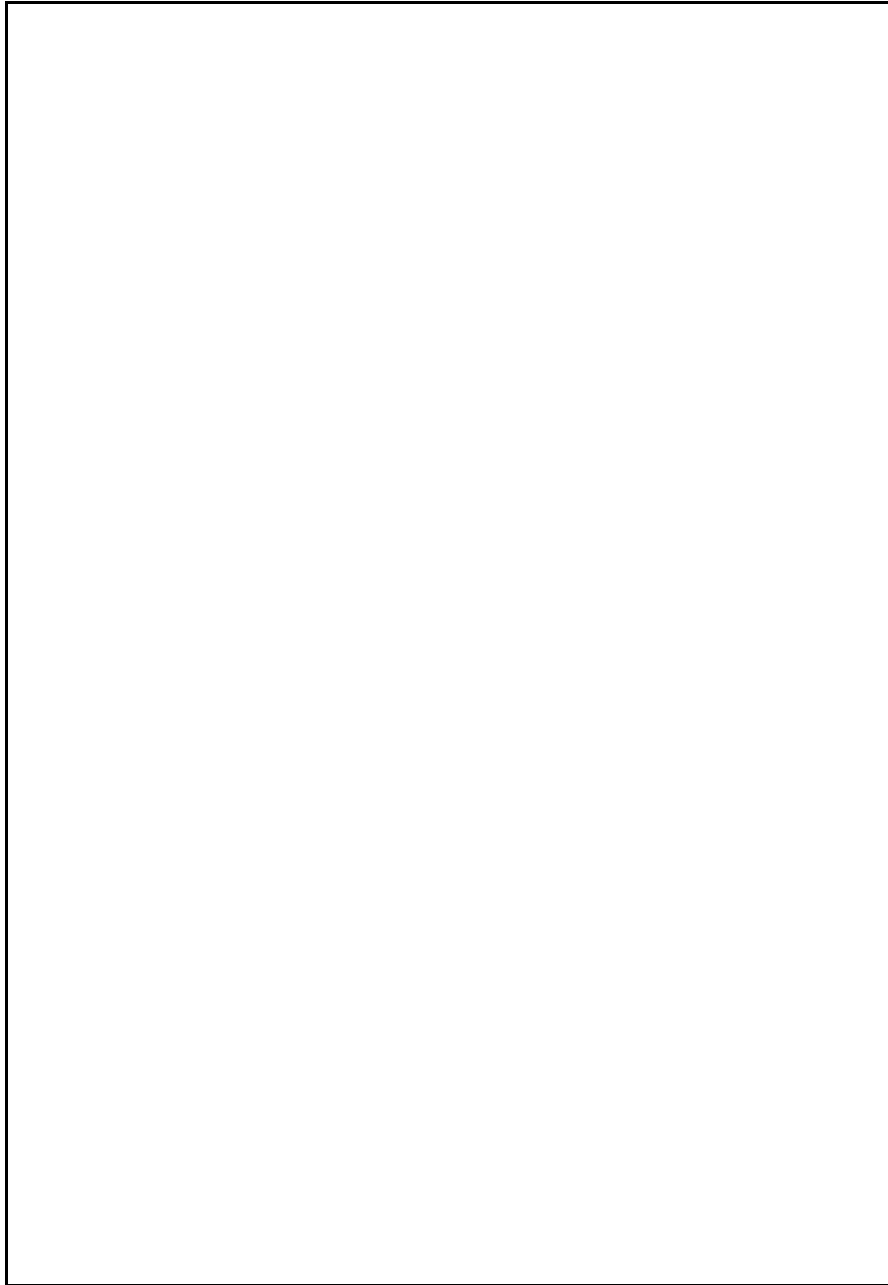


Illustration 4.1. UV-scan of a letter written in urine by a detainee. The revealed text appeared to contain very incriminating evidence. [source: Stapel & De Koning, 216]

One other problem deserves mentioning, as it involves cryptography-related technologies. Electronic cash can be used for sending large amounts of money around the world in a very short period, as often as is desirable. This is a great opportunity for money laundering, as tracing all these transactions is virtually impossible. Since financial investigation has become an important part of investigating organized crime, e-cash poses a serious problem to laying bare the financial patterns of a criminal organization. This problem, however, is outside the scope of this book.

4.5.5. Scope of the problem

The publicly available information, in particular the Denning-Baugh survey, suggests that cryptography is encountered in only a few criminal cases. Where encryption is encountered, it often does not block the investigation, either because the police can crack it or because there is sufficient other evidence.

In *telecommunications*, end-to-end cryptography is used little by criminals.⁵⁴ If they do, investigation usually stands powerless. Encryption is used more often in protecting *stored* criminal data, but in quite a few of the crypto-cases to date, the investigators were able to crack the encryption or the encrypted data were not necessary for a conviction. Only a small group of criminals use robust cryptography which cannot be cracked, and where practical attacks do not work. The Walsh report on Australian crypto policy corroborates this: "For the present, the investigative capability of the agencies is not significantly affected." [Walsh, 1.2.11] The threat, then, of cryptocriminals to law enforcement is presently a minor one.

The general expectation, however, is that the cryptocriminal threat will grow significantly in the near to middle future.⁵⁵ The central claim of the Denning-Baugh study is "that the impact of encryption on crime and terrorism is at its early stages." [Denning 97a] As cryptography becomes familiar to ever wider groups of users, also less technologically advanced criminals will start to use robust cryptography. The profoundest impact will likely result from incorporating strong cryptography in general software programs, such as word-processing, browsing, and e-mail software. US export controls still curb this development, but it seems inevitable that the information infrastructure and the primary information services will incorporate strong cryptography in the near future. Then, investigation will still benefit from practical attacks exploiting weaknesses in the use of cryptography, but cracking or brute-forcing of weak crypto systems employed by criminals will be a thing of the past.

4.6. Conclusion

Developments in crime show that organized crime and computer crime have become serious threats to society. Both are dependent on information-processing: criminal organizations rely heavily on communications, and computer criminals often use data storage. Both criminal

54 "As far as the committee has been able to determine, criminal use of digitally encrypted voice communications has not presented a significant problem to law enforcement to date." [NRC, 90]

55 For instance, [COM (97) 503, III.3(I)], [Denning 97a], [Australia, 6], [Norway, 2], and Interpol expert Takizawa in [Ghosh].

organizations and computer criminals use modern technologies, and are likely to use these to shield their activities from police scrutiny. Business crime, including large-scale fraud, also relies on data storage and may use encryption to hide incriminating evidence. Other forms of serious crime can also involve data transport or storage.

To counter the threats of serious crime, states investigate crime and prosecute the perpetrators. To assure the safety of citizens and the integrity of society as a whole, investigation and prosecution are of great concern. The Dutch Minister of Justice has called fighting organized crime and other serious forms of crime a “pressing social need” [23047, nr 3, 3].

In investigating these types of crime, information-gathering has a central place. Wiretaps and traffic analysis are primary tools for revealing structures of criminal organizations and for tracing hackers. Technological developments are making tapping more difficult, in particular of mobile phones and electronic data transfers. The obligation for telecom operators to make their networks tappable may require several years to take full effect. Search and seizure, including specific powers for investigating in automated surroundings, are main methods of gathering evidence and tracing computer crime and business crime.

Currently, encryption is used very little by criminals in *telecommunications*; if they do, however, it is generally impossible for the police to retrieve the contents of the communications. At present, the technical problems of tapping all forms of communications are more serious than the use of cryptography, but once tapping all telecommunications is widely possible, cryptography is bound to render taps useless. Wiretaps will become illusory if criminals regularly encrypt end-to-end. The extent to which criminals will do this is hard to predict, but one can safely assume that it will rise, especially where communications via the computer (e-mail, Internet telephony) are concerned. Gathering information *about* the communications data is not hampered by cryptography, and so, traffic analysis will remain an important tool for investigation.

Cryptocriminals today are using cryptography oftener in *data storage*. So far, this usually does not hamper the investigation, because the police can crack the ciphertext or because there is sufficient other evidence. However, with the developing information infrastructure, robust cryptography will come within the easy reach of more criminals (in particular, of less-automated organized criminals and of business and computer criminals who currently do not use encryption, or who use it insecurely). Although significant opportunities may remain for the police to crack encryption by exploiting weaknesses in crypto use if not in crypto systems, overall, searches in computers will become ever less effective.

I conclude that the threat of cryptography to law enforcement, and therewith to society at large, is currently low, as there are few real cryptocriminals to date. The threat, however, will increase in the near to middle future. Therefore, there is a significant public concern to address the crypto problems for law enforcement.

The main crypto problems for law enforcement

Problem 1: criminals' use of strong confidentiality encryption for voice and data transport

Problem 1a: criminals' use of steganography to hide communications

Problem 2: criminals' use of strong confidentiality encryption for data storage

Problem 2a: criminals' use of steganography to hide data in storage

Problem 2b: criminals' use of duress codes to decrypt to a different message