EUROPEAN PARLIAMENT

1999 *2004*

Temporary Committee on the ECHELON Interception System

PROVISIONAL

18 May 2001

DRAFT REPORT

on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)

Temporary Committee on the ECHELON Interception System

Rapporteur: Gerhard Schmid

CONTENTS

Page

PROCEDURAL PAGE

At the sitting of 5 July 2001 the European Parliament decided to set up a Temporary Committee on the ECHELON Interception System. With a view to fulfilling its mandate, at its constituent meeting of 9 July 2000 the Temporary Committee appointed Gerhard Schmid rapporteur.

At its meeting(s) of … the committee considered the draft report.

The following were present for the vote: ... chairman/acting chairman; ... and ..., vice-chairman/vice-chairmen; ..., rapporteur; ..., ... (for ...), ... (for ... pursuant to Rule 153(2)), ... and ... .

The report was tabled on ....

The deadline for tabling amendments will be indicated in the draft agenda for the relevant part-session.

MOTION FOR A RESOLUTION

European Parliament resolution on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)

The European Parliament,

– having regard to Parliament's decision of 5 July 2000 to set up a Temporary Committee on the ECHELON Interception System and the mandate issued to the Temporary Committee,

– having regard to the EC Treaty, one objective of which is the establishment of a common market with a high level of competitiveness,

– having regard to the Treaty on European Union, in particular Article 6(2) thereof, which lays down the requirement that the EU must respect fundamental rights, and Title V thereof, which sets out provisions governing the common foreign and security policy,

– having regard to the Charter of Fundamental Rights of the EU, Article 7 of which lays down the right to respect for private and family life and explicitly enshrines the right to respect for communications,

– having regard to the European Convention on Human Rights (ECHR), in particular Article 8 thereof, which governs the protection of private life, and the many other international conventions which provide for the protection of privacy,

– having regard to the report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) drawn up by the Temporary Committee on the ECHELON Interception System (A5-…./2001),

The existence of a global system for intercepting private and commercial communications (the ECHELON interception system)

A. whereas the existence of a global system for intercepting communications, operating by means of cooperation proportionate to their capabilities among the USA, the UK, Canada, Australia and New Zealand under the UKUSA Agreement, is no longer in doubt; whereas it seems likely, in view of the evidence, that its name is in fact ECHELON, although this is a relatively minor detail,

B. whereas the purpose of the system is to intercept private and commercial communications, and not military communications, although the analysis carried out in the report has revealed that the system cannot be nearly as extensive as some sections of the media have assumed,

The limits of the interception system

C. whereas the surveillance system depends upon worldwide interception of satellite communications, although in areas characterised by a high volume of communications only a very small proportion of those communications are transmitted by satellite; whereas this means that the majority of communications cannot be intercepted by earth stations, but

only by tapping cables and intercepting radio signals, something which - as the investigations carried out in connection with the report have shown - is possible only to a limited extent; whereas the numbers of personnel required for the final analysis of intercepted communications imposes further restrictions; whereas, therefore, the ECHELON states have access to only a very limited proportion of cable and radio communications and can analyse only a limited proportion of those communications,

The possible existence of other interception systems

D. whereas the interception of communications is a method of spying commonly employed by intelligence services, so that other states might also operate similar systems, provided that they have the required funds and the right locations; whereas geographically at least – thanks to its overseas territories – France is the only EU Member State which could set up a global interception system by itself, and whereas there is also evidence that Russia might likewise be able to operate such a system,

Compatibility with EU law

E. whereas, as regards the question of the compatibility of a system of the ECHELON type with EU law, it is necessary to distinguish between two scenarios: if a system is used purely for intelligence purposes, there is no violation of EU law, since operations in the interests of state security are not subject to the EC Treaty, but would fall under Title V of the Treaty on European Union (CFSP), although at present that title lays down no provisions on the subject, so that no criteria are available; if, on the other hand, the system is abused for the purposes of gathering competitive intelligence, such action is at odds with the Member States' duty of loyalty and with the concept of a common market based on free competition, so that a Member State participating in such a system violates EC law,

Compatibility with the fundamental right to respect for private life (Article 8 of the ECHR)

F. whereas any interception of communications represents serious interference with an individual's exercise of the right to privacy; whereas Article 8 of the ECHR, which guarantees respect for private life, permits interference with the exercise of that right only in the interests of national security, in so far as this is in accordance with domestic law and the provisions in question are generally accessible and lay down under what circumstances, and subject to what conditions, the state may undertake such interference; whereas interference must be proportionate, so that competing interests need to be weighed up and, under the terms of the case law of the European Court of Human Rights, it is not enough that the interference should merely be useful or desirable,

G. whereas an intelligence system which intercepted all communications without any guarantee of compliance with the principle of proportionality would not be compatible with the ECHR; whereas it would also constitute a violation of the ECHR if the rules governing the surveillance of communications lacked a legal basis, if the rules were not generally accessible or if they were so formulated that their implications for the individual were unforeseeable; whereas most of the rules governing the activities of US intelligence services abroad are classified, so that compliance with the principle of proportionality is at least doubtful and breaches of the principles of accessibility and forseeability laid down by the European Court of Human Rights probably occur,

H. whereas the Member States cannot circumvent the requirements imposed on them by the ECHR by allowing other countries' intelligence services, which are subject to less stringent legal provisions, to work on their territory, since otherwise the principle of legality, with its twin components of accessibility and forseeability, would become a dead letter and the case law of the European Court of Human Rights would be deprived of its substance,

I. whereas, in addition, the lawful operations of intelligence services are consistent with fundamental rights only if adequate arrangements exist for monitoring them, in order to counterbalance the risks inherent in secret activities performed by a part of the administrative apparatus; whereas the European Court of Human Rights has expressly stressed the importance of an efficient system for monitoring intelligence operations, so that there are grounds for concern in the fact that some Member States do not have parliamentary monitoring bodies of their own responsible for scrutinising the secret services,

Are EU citizens adequately protected against intelligence services?

J. whereas the protection enjoyed by EU citizens depends on the legal situation in the individual Member States, which varies very substantially, and whereas in some cases parliamentary monitoring bodies do not even exist, so that the degree of protection can hardly be said to be adequate; whereas it is in the fundamental interests of European citizens that their national parliaments should have a specific, formally structured monitoring committee responsible for supervising and scrutinising the activities of the intelligence services; whereas even where monitoring bodies do exist, there is a strong temptation for them to concentrate more on the activities of domestic intelligence services, rather than those of foreign intelligence services, since as a rule it is only the former which affect their own citizens,

K. whereas, in the event of cooperation between intelligence services under the CFSP, the institutions must introduce adequate measures to protect European citizens,

Industrial espionage

L. whereas part of the remit of foreign intelligence services is to gather economic data, such as details of developments in individual sectors of the economy, trends on commodity markets, compliance with economic embargoes, observance of rules on supplying dual-use goods, etc., and whereas, for these reasons, the firms concerned are often subject to surveillance,

M. whereas the situation becomes intolerable when intelligence services allow themselves to be used for purposes of gathering competitive intelligence by spying on foreign firms with the aim of securing a competitive advantage for firms in the home country, and whereas it is frequently maintained that the global interception system has been used in this way, although no such case has been substantiated,

N. whereas sensitive commercial data are mostly kept inside individual firms, so that competitive intelligence-gathering primarily involves efforts to obtain information through members of staff or through people planted in the firm for this purpose or else by hacking

into internal computer networks; whereas only if sensitive data are transmitted externally by cable or radio (satellite) can a communications surveillance system be used for competitive intelligence-gathering; whereas this applies systematically in the following three cases:
- in the case of firms which operate in three time zones, so that interim results are sent from Europe to America and on to Asia;
- in the case of videoconferencing within multinationals using VSAT or cable;
- if vital contracts are being negotiated on the spot (e.g. for the building of plants, telecommunications infrastructure, the creation of new transport systems, etc.) and it is necessary to consult the firm's head office,

Possible self-protection measures

O. whereas firms can only make themselves secure by safeguarding their entire working environment and protecting all communications channels which are used to send sensitive information; whereas sufficiently secure encryption systems exist at affordable prices on the European market; whereas private individuals should also be urged to encrypt e-mails; whereas an unencrypted e-mail message is like a letter without an envelope; whereas relatively user-friendly systems exist on the Internet which are even made available for private use free of charge,

Cooperation among intelligence services within the EU

P. whereas the EU has reached agreement on the coordination of intelligence-gathering by intelligence services as part of the development of its own security and defence policy, although cooperation with other partners in these areas will continue,

Q. whereas cooperation among intelligence services within the EU seems desirable on the grounds that, firstly, a common security policy which did not involve the secret services would not make sense, and, secondly, it would have numerous professional, financial and political advantages; whereas it would also accord better with the idea of the EU as a partner on an equal footing with the United States and could bring together all the Member States in a system which complied fully with the ECHR; whereas the European Parliament would of course have to exercise appropriate monitoring,

R. whereas the European Parliament is in the process of drawing up its own rules concerning access to confidential and sensitive information and documents,

Conclusion and amendment of international agreements on the protection of citizens and firms

1. Calls on the Secretary-General of the Council of Europe to submit to the Ministerial Committee an analysis of whether the protection of private life guaranteed in Article 8 of the ECHR should be brought into line with modern communication and interception methods by means of an additional protocol or, together with the provisions governing data protection, as part of a revision of the Convention on Data Protection, with the proviso that this should neither undermine the level of legal protection established by the European Court of Human Rights nor reduce the flexibility which is vital if future developments are to be taken into account;

2. Calls on the Member States to establish a European platform in order to review the legal provisions guaranteeing postal and communications secrecy and, in addition, to reach agreement on a joint text which affords all European citizens, throughout the territory of the Member States, protection of privacy as defined in Article 7 of the Charter of Fundamental Rights of the European Union and which, moreover, guarantees that the activities of intelligence services are carried out in a manner consistent with fundamental rights, in keeping with the conditions set out in Chapter 8 of this report, and in particular Section 8.3.4., as derived from Article 8 of the ECHR;

3. Calls on the member countries of the Council of Europe to adopt an additional protocol which enables the European Communities to accede to the ECHR or to consider other measures designed to prevent disputes relating to case law arising between the European Court of Human Rights and the Court of Justice of the European Communities;

4. Calls on the UN Secretary-General to instruct the competent committee to put forward proposals designed to bring Article 17 of the International Covenant on Civil and Political Rights, which guarantees the protection of privacy, into line with technical innovations;

5. Calls on the USA to sign the Additional Protocol to the International Covenant on Civil and Political Rights, so that complaints by individuals concerning breaches of the Covenant by the USA can be submitted to the Human Rights Committee set up under the Covenant; calls on the relevant American NGOs, in particular the ACLU (American Civil Liberties Union) and the EPIC (Electronic Privacy Information Center), to exert pressure on the US Administration to that end;

National legislative measures to protect citizens and firms

6. Calls on the Member States to review their own legislation on the operations of the intelligence services to ensure that it is consistent with fundamental rights;

7. Calls on the Member States to aspire to a common level of protection against intelligence operations based on the highest level of protection which exists in any Member State, since as a rule it is citizens of other states, and hence also of other Member States, that are affected by the operations of foreign intelligence services;

8. Calls on the EU institutions, in the event of cooperation between intelligence services under the CFSP, to introduce adequate measures to protect European citizens; the European Parliament, as the logical monitoring body, must for its part create the preconditions for the supervision of this highly sensitive area in order to make it realistic – and indeed defensible – to insist on being granted the necessary monitoring rights;

Specific legal measures to combat industrial espionage

9. Calls on the Member States to consider to what extent industrial espionage and the payment of bribes as a means of securing contracts can be combated by means of European and international legal provisions and, in particular, whether WTO rules could be adopted which take account of the distortions of competition brought about by such practices, for example by rendering contracts obtained in this way null and void;

10. Calls on the Member States to undertake by means of a clear joint declaration not to engage in industrial espionage against one another, thereby signifying their compliance with the letter and spirit of the EC Treaty;

Measures concerning the implementation of the law and the monitoring of that implementation

11. Calls on the national parliaments which have no parliamentary monitoring body responsible for scrutinising the activities of the intelligence services to set up such a body;

12. Calls on the monitoring bodies responsible for scrutinising the activities of the secret services, when exercising their monitoring powers, to attach great importance to the protection of privacy, regardless of whether the individuals concerned are their own nationals, other EU nationals or third-country nationals;

13. Calls on Germany and England to make the authorisation of further communications interception operations by US intelligence services on their territory conditional on their compliance with the ECHR, i.e. to stipulate that they should be consistent with the principle of proportionality, that their legal basis should be accessible and that the implications for individuals should be foreseeable, and to introduce corresponding, effective monitoring measures, since they are responsible for ensuring that intelligence operations authorised or even merely tolerated on their territory respect human rights;

Measures to encourage self-protection by citizens and firms

14. Calls on the Commission and Member States to develop programmes to foster awareness of security problems among citizens and firms and at the same time to provide practical assistance in designing and implementing comprehensive protection strategies;

15. Urges the Commission and Member States to devise appropriate measures to promote, develop and manufacture European encryption technology and software and above all to support projects aimed at developing user-friendly open-source encryption software;

16. Calls on the Commission and Member States to promote software projects whose source text is made public (open-source software), as this is the only way of guaranteeing that no backdoors are built into programmes;

17. Calls on the European institutions and the public administrations of the Member States systematically to encrypt e-mails, so that ultimately encryption becomes the norm;

Other measures

18. Calls on firms to cooperate more closely with counter-espionage services, and particularly to inform them of attacks from outside for the purposes of industrial espionage, in order to improve the services' efficiency;

19. Calls on the Commission to put forward a proposal to set up a European advisory centre to deal with issues relating to the security of the information held by firms, with the twin task of increasing awareness of the problem and providing practical assistance;

20. Takes the view that an international congress on the protection of privacy against telecommunications surveillance should be held in order to provide NGOs from Europe, the USA and other countries with a forum for discussion of the cross-border and international aspects of the problem and coordination of areas of activity and action;

21. Instructs its President to forward this resolution to the Council, the Commission, the governments and parliaments of the Member States and applicant countries and the Council of Europe.

EXPLANATORY STATEMENT

1. Introduction

1.1. The reasons for setting up the committee

On 5 July 2000 the European Parliament decided to set up a temporary committee on the ECHELON system. This step was prompted by the debate on the study commissioned by STOA[1] concerning the so-called ECHELON system[2], which the author, Duncan Campbell, had presented at a hearing of the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs on the subject 'the European Union and data protection'.

1.2. The claims made in the two STOA studies on a global interception system codenamed ECHELON

1.2.1. The first STOA report of 1997

A report which STOA[3] commissioned from the Omega Foundation for the European Parliament in 1997 on 'An Appraisal of Technologies of Political Control' described ECHELON in a chapter concerning 'national and international communications interception networks'. The author claimed that all e-mail, telephone and fax communications in Europe were routinely intercepted by the US National Security Agency[4]. As a result of this report, the alleged existence of a comprehensive global interception system called ECHELON was brought to the attention of people throughout Europe.

1.2.2. The 1999 STOA reports

In 1999, in order to find out more about this subject, STOA commissioned a five-part study of the 'development of surveillance technology and risk of abuse of economic information'. Part 2/5, by Duncan Campbell, concerned the existing intelligence capacities and particularly the mode of operation of ECHELON[5].

Concern was aroused in particular by the assertion in the report that ECHELON had moved away from its original purpose of defence against the Eastern Bloc and was currently being used for purposes of industrial espionage. Examples of alleged industrial espionage were given in support of the claim: in particular, it was stated that Airbus and Thomson CFS had been damaged as a result.

---

[1] STOA (Scientific and Technological Options Assessment) is a department of the Directorate-General for Research of the European Parliament which commissions research.
[2] The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems and its applicability to COMINT targeting and selection, including speech recognition (October 1999).
[3] Scientific and Technological Options Assessment
[4] Steve Wright, An appraisal of technologies of political control (1998), 20
[5] The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems and its applicability to COMINT targeting and selection, including speech recognition (October 1999), PE 168.184.

As a result of the STOA study, ECHELON was debated in the parliaments of virtually all the Member States; in France and Belgium, reports were even drafted on it.

1.3. The mandate of the committee

At the same time as it decided to set up a temporary committee, the European Parliament drew up its mandate. It reads as follows:

- '- to verify the existence of the communications interception system known as ECHELON, whose operation is described in the STOA report published under the title "Development of surveillance technology and risks of abuse of economic information";
- - to assess the compatibility of such a system with Community law, in particular Article 286 of the EC Treaty and Directives 95/46/EC and 97/66/EC, and with Article 6(2) of the EU Treaty, in the light of the following questions:
    - - are the rights of European citizens protected against activities of secret services?
    - - is encryption an adequate and sufficient protection to guarantee citizens' privacy or should additional measures be taken and if so what kind of measures?
    - - how can the EU institutions be made better aware of the risks posed by these activities and what measures can be taken?
- - to ascertain whether European industry is put at risk by the global interception of communications;
- - possibly, to make proposals for political and legislative initiatives.'

1.4. Why not a committee of inquiry?

The European Parliament decided to set up a temporary committee because it is possible to set up a committee of inquiry only to investigate violations of Community law under the EC Treaty (Article 193 TEC), and such committees can accordingly only consider matters governed by it. Matters falling under Titles V (Common Foreign and Security Policy) and VI (Police and Judicial Cooperation in Criminal Matters) of the Treaty on European Union are excluded. Moreover, under the interinstitutional decision[1] the special powers of a committee of inquiry to call people to appear and to inspect documents apply only if grounds of secrecy or public or national security do not dictate otherwise, which would certainly make it impossible to summon secret services to appear. Furthermore, a committee of inquiry cannot extend its work to third countries, because by definition the latter cannot violate EU law. Thus, setting up a committee of inquiry would only have restricted the scope of any investigations opening up any additional rights, for which reason the idea was rejected by a majority of Members of the European Parliament.

1.5. Working method and schedule

With a view to carrying out its mandate in full, the committee decided to proceed in the following way. A programme of work proposed by the rapporteur and adopted by the committee

[1] Decision of the European Parliament, the Council and the Commission of 19 April 1995 on the detailed provisions governing the exercise of the European Parliament's right of inquiry (95/167/EC), Article 3(3)-(5).

listed the following relevant topics: 1. Certain knowledge about ECHELON, 2. Debate by national parliaments and governments, 3. Intelligence services and their operations, 4. Communications systems and the scope for intercepting them, 5. Encryption, 6. Industrial espionage, 7. Aims of espionage and protective measures, and 8. Legal context and protection of privacy. The topics were considered consecutively at the individual meetings, the order of consideration being based on practical grounds and thus not implying anything about the value assigned to the individual topics. By way of preparation for the meetings, the rapporteur systematically scrutinised and evaluated the material available. At the meetings, in accordance with the requirements of the topic concerned, representatives of national administrations (particularly secret services) and parliaments in their capacity as bodies responsible for monitoring secret services were invited to attend, as were legal experts and experts in the fields of communications and interception technology, business security and encryption technology with both academic and practical backgrounds. Journalists who had investigated this field were also heard. The meetings were generally held in public, although some sessions were also held behind closed doors where this was felt to be advisable in the interests of obtaining information. In addition, the chairman of the committee and the rapporteur visited London and Paris together to meet people who for a wide variety of different reasons were unable to attend meetings of the committee but whose involvement in the committee's work nonetheless seemed advisable. For the same reasons, the committee's bureau, the coordinators and the rapporteur travelled to the USA. The rapporteur also held many one-to-one talks, in some cases in confidence.

1.6. Characteristics ascribed to the ECHELON system

The system known as 'ECHELON' is an interception system which differs from other intelligence systems in that it possesses two features which make it quite unusual:

The first such feature attributed to it is the capacity to carry out quasi-total surveillance. Satellite receiver stations and spy satellites in particular are alleged to give it the ability to intercept any telephone, fax, Internet or e-mail message sent by any individual and thus to inspect its contents.

The second unusual feature of ECHELON is said to be that the system operates worldwide on the basis of cooperation proportionate to their capabilities among several states (the UK, the USA, Canada, Australia and New Zealand), giving it an added value in comparison to national systems: the states participating in ECHELON (ECHELON states) can place their interception systems at each other's disposal, share the cost and make joint use of the resulting information. This type of international cooperation is essential in particular for the worldwide interception of satellite communications, since only in this way is it possible to ensure in international communications that both sides of a dialogue can be intercepted. It is clear that, in view of its size, a satellite receiver station cannot be established on the territory of a state without that state's knowledge. Mutual agreement and proportionate cooperation among several states in different parts of the world is essential.

Possible threats to privacy and to businesses posed by a system of the ECHELON type arise not only from the fact that is a particularly powerful monitoring system, but also that it operates in a largely legislation-free area. Systems for the interception of international communications are not usually targeted at residents of the home country. The person whose messages were intercepted would have no domestic legal protection, not being resident in the country concerned. Such a person would be completely at the mercy of the system. Parliamentary

supervision would also be inadequate in this area, since the voters, who assume that interception 'only' affects people abroad, would not be particularly interested in it, and elected representatives chiefly follow the interests of their voters. That being so, it is hardly surprising that the hearings held in the US Congress concerning the activities of the NSA were confined to the question of whether US citizens were affected by it, with no real concern expressed regarding the existence of such a system in itself. It thus seems all the more important to investigate this issue at European level.

2. The operations of foreign intelligence services

2.1. Introduction

In addition to police forces, most governments run intelligence services to protect their country's security. As their operations are generally secret, they are also referred to as secret services. These services have the following tasks:

- gathering information to avert dangers to state security
- counter-espionage in general
- averting possible dangers to the armed forces
- gathering information about situations abroad.

2.2. What is espionage?

Governments have a need for systematic collection and evaluation of information about certain situations in other states. This serves as a basis for decisions concerning the armed forces, foreign policy and so on. They therefore maintain foreign intelligence services, part of whose task is to systematically assess information available from public sources. The rapporteur has been informed that on average this accounts for at least 80% of the work of the intelligence services.[1] However, particularly significant information in the fields concerned is kept secret from governments or businesses and is therefore not publicly accessible. Anyone who nonetheless wishes to obtain it has to steal it. Espionage is simply the organised theft of information.

2.3. Espionage targets

The classic targets of espionage are military secrets, other government secrets or information concerning the stability of or dangers to governments. These may for example comprise new weapons systems, military strategies or information about the stationing of troops. No less important is information about forthcoming decisions in the fields of foreign policy, monetary decisions or inside information about tensions within a government. In addition there is also interest in economically significant information. This may include not only information about sectors of the economy but also details of new technologies or foreign transactions.

2.4. Espionage methods

Espionage involves gaining access to information which the holder would rather protect from being accessed by outsiders. This means that the protection needs to be overcome and penetrated. This is the case with both political and industrial espionage. Thus the same problems arise with espionage in both fields, and the same techniques are accordingly used in both of them. Logically speaking there is no difference, only the level of protection is generally lower in the economic sphere, which sometimes makes it easier to carry out industrial espionage. In

[1] The Commission on the Roles and Capabilities of the US Intelligence Community has stated in its report 'Preparing for the 21st Century: An Appraisal of US Intelligence' that 95% of all economic intelligence is derived from open sources (Chapter 2, 'The Role of Intelligence').

particular, businessmen tend to be less aware of risks when using interceptible communication media than does the state when employing them in fields where security is a concern.

2.4.1. Human intelligence

Protection of secret information is always organised in the same way:
- only a small number of people, who have been vetted, have access to secret information
- there are established rules for dealing with such information
- normally the information does not leave the protected area, and if it does so, it leaves only in a secure manner or encrypted form. The prime method of carrying out organised espionage is therefore by gaining access to the desired information directly through **people** ('human intelligence'). These may be:
  - plants (agents) acting on behalf of the service/business engaging in espionage
  - people recruited from the target area.

Recruits generally work for an outside service or business for the following reasons:
- sexual seduction
- bribery in cash or in kind
- blackmail
- ideological grounds
- attachment of special significance or honour to a given action (playing on dissatisfaction or feelings of inferiority).

A borderline case is unintentional cooperation by means of which information is 'creamed off'. This involves persuading employees of authorities or businesses to disclose information in casual conversation, for example by exploiting their vanity, under apparently harmless circumstances (through informal contact at conferences or trade fairs or in hotel bars).

The use of people has the advantage of affording direct access to the desired information. However, there are also disadvantages:
- counter-espionage always concentrates on people or controlling agents
- where an organisation's staff are recruited, the weaknesses which laid them open to recruitment may rebound on the recruiting body
- people always make mistakes, which means that sooner or later they will be detected through counter-espionage operations.

Where possible, therefore, organisations try to replace the use of agents or recruits with non-human espionage. This is easiest in the case of the analysis of radio signals from military establishments or vehicles.

2.4.2. Processing of electromagnetic signals

The form of espionage by technical means with which the public are most familiar is that which uses satellite photography. In addition, however, electromagnetic signals of any kind are intercepted and analysed ('signals intelligence', SIGINT).

2.4.2.1. Electromagnetic signals used for non-communication purposes

In the military field, certain electromagnetic signals, e.g. those from radar stations, may provide valuable information about the organisation of enemy air defences ('electronic intelligence', ELINT). In addition, electromagnetic radiation which could reveal details of the position of troops, aircraft, ships or submarines is a valuable source of information for an intelligence service. Monitoring other states' spy satellites which take photographs, and recording and decoding signals from such satellites, is also useful.

The signals are recorded by ground stations, from low-orbit satellites or from quasi-geostationary SIGINT satellites. This aspect of intelligence operations using electromagnetic means consumes a large part of services' interception capacity. However, this is not the only use made of technology.

2.4.2.2. Processing of intercepted communications

The foreign intelligence services of many states intercept the military and diplomatic communications of other states. Many of these services also monitor the civil communications of other states if they have access to them. In some states, services are also authorised to monitor incoming or outgoing communications in their own country. In democracies, intelligence services' monitoring of the communications of the country's **own** citizens is subject to certain triggering conditions and controls. However, domestic law only protects citizens within the territory of their own country (see Chapter 8).

2.5. The operations of certain intelligence services

Public debate has been sparked primarily by the interception operations of the American and British intelligence services. They have been criticised for recording and analysing communications (voice, fax, e-mail). A **political** assessment requires a yardstick for judging such operations. The interception operations of foreign intelligence services in the EU may be taken as a basis for comparison. Table 1 provides an overview. This shows that interception of private communications by foreign intelligence services is by no means confined to the American or British foreign intelligence services.

Country	Communications in foreign countries	State communications	Civilian communications
Belgium	+	+	-
Denmark	+	+	+
Finland	+	+	+

France	+	+	+
Germany	+	+	+
Greece	+	+	-
Ireland	-	-	-
Italy	+	+	+
Luxembourg	-	-	-
Netherlands	+	+	+
Austria	+	+	-
Portugal	+	+	-
Sweden	+	+	+
Spain	+	+	+
UK	+	+	+
USA	+	+	+
Canada	+	+	+
Australia	+	+	+
New Zealand	+	+	+

Table 1: Interception operations by intelligence services in the EU and in the ECHELON states

The columns refer to:

Column 1: The country concerned

Column 2: Communications in foreign countries intercepted

Column 3: State communications (military, embassies, etc.) intercepted

Column 4: Civilian communications intercepted

3. Technical conditions governing the interception of telecommunications

3.1. The interceptibility of various communication media

If people wish to communicate with one another over a given distance, they need a medium. This medium may be:

- air (sound waves)
- light (Morse lamp, fibreoptic cable)
- electric current (telegraph, telephone)
- an electromagnetic wave (all forms of radio).

Any third party who succeeds in accessing the medium can intercept the communications. This process may be easy or difficult, feasible anywhere or only from certain locations. Two extreme cases are discussed below: the technical possibilities available to a spy working on the spot, on the one hand, and the scope for a worldwide interception system, on the other.

3.2. The scope for interception on the spot[1]

On the spot, any form of communication can be intercepted if the eavesdropper is prepared to break the law and the target does not take protective measures.

- **Conversations** in rooms can be intercepted by means of planted microphones (bugs) or laser equipment which picks up vibrations in window panes.

- **Screens** emit radiation which can be picked up at a distance of up to 30 metres, revealing the information on the screen.

- **Telephone, fax, and e-mail messages** can be intercepted if the eavesdropper taps into a cable leaving the relevant building.

- Communications from a **mobile phone** can be intercepted at a distance of up to …. km.

- **Closed-circuit communications** can be intercepted within the USW-radio range.

Conditions for the use of espionage equipment are ideal on the spot, since the interception measures can be focused on one person or one target and almost every communication can be intercepted. The only disadvantage may be the risk of detection in connection with the planting of bugs or the tapping of cables.

[1] Manfred Fink, Eavesdropping on the economy – Interception risks and techniques – prevention and protection, Richard Boorberg Verlag, Stuttgart, 1996.

3.3. The scope for a worldwide interception system

Today, various media are available for all forms of intercontinental communication (voice, fax and data). The scope for a worldwide interception system is restricted by two factors:

- restricted access to the communication medium
- the need to filter out the relevant communication from a huge mass of communications taking place at the same time.

3.3.1. Access to communication media

3.3.1.1. Cable communications

All forms of communication (voice, fax, e-mail, data) are transmitted by cable. Access to the cable is a prerequisite for the interception of communications of this kind. Access is certainly possible if the terminal of a cable connection is situated on the territory of a state which allows interception. **In technical terms**, therefore, within an individual state all communications carried by cable can be intercepted, provided this is permissible under the law. However, foreign intelligence services generally have no legal access to cables situated on the territory of other states. At best, they can gain illegal access to a specific cable, although the risk of detection is high.

From the telegraph age onwards, intercontinental cable connections have been achieved by means of underwater cables. Access to these cables is always possible at those points where they emerge from the water. If several states join forces to intercept communications, access is possible to all the terminals of the cable connections situated in those states. This was historically significant, since both the underwater telegraph cables and the first underwater coaxial telephone cables linking Europe and America landed in Newfoundland and the connections to Asia ran via Australia, because regenerators were required. Today, fibreoptic cables follow the direct route, regardless of the mountainous nature of the oceanbed and the need for regenerators, and do not pass via Australia or New Zealand.

Electric cables may also be tapped between the terminals of a connection, by means of induction (i.e. electromagnetically, by attaching a coil to the cable), without creating a direct, conductive connection. Underwater electric cables can also be tapped in this way from submarines, albeit at very high cost. This technique was employed by the USA in order to tap into a particular underwater cable laid by the USSR to transmit unencrypted commands to Soviet atomic submarines. The high costs alone rule out the comprehensive use of this technique.

In the case of the older-generation fibreoptic cables used today, inductive tapping is only possible at the regenerators. These regenerators transform the optical signal into an electrical signal, strengthen it and then transform it back into an optical signal. However, this raises the issue of how the enormous volumes of data carried on a cable of this kind can be transmitted from the point of interception to the point of evaluation without the laying of a separate fibreoptic cable. On cost grounds, the use of a submarine fitted with processing equipment is conceivable only in very rare cases, for example in wartime, with a view to intercepting the enemy's strategic military communications. In your rapporteur's view, the use of submarines for

the routine surveillance of international telephone traffic can be ruled out. The new-generation fibreoptic cables use erbium lasers as regenerators – interception by means of electromagnetic coupling is thus no longer possible! Communications transmitted using fibreoptic cables of this kind can thus only be intercepted at the terminals of the connection.

The practical implication for the **ECHELON states** (the alliance formed for the purposes of interception) is that communications can be intercepted at acceptable cost only at the terminals of the underwater cables which land on their territory. Essentially, therefore, they can only tap incoming or outgoing cable communications! In other words, their access to cable communications **in Europe** is restricted to **the territory of the United Kingdom**, since hitherto internal communications have mostly been transmitted via the domestic cable network. The privatisation of telecommunications may give rise to exceptions, but these are specific and unpredictable!

This is valid at least for telephone and fax communications. Other conditions apply to communications transmitted over the Internet via cable. The situation can be summarised as follows:

- Internet communications are carried out using data packets and different packets addressed to the same recipient may take different routes through the network.

- At the start of the Internet age, spare capacity in the public network was used for the transmission of e-mail communications. For that reason, the routes followed by individual data packets were completely unpredictable and arbitrary. At that time, the most important international connection was the 'science backbone' between Europe and America.

- The commercialisation of the Internet and the establishment of Internet providers also resulted in a commercialisation of the network. Internet providers operated or rented their own networks. They therefore made increasing efforts to keep communications within their own network in order to avoid paying user fees to other operators. Today, the route taken through the network by a data packet is therefore not solely determined by the capacity available on the network, but also hinges on costs considerations.

- An e-mail sent from a client of one provider to a client of another provider is generally routed through the firm's network, even if this is not the quickest route. Routers, computers situated at network junctions and which determine the route by which data packets will be transmitted, organise the transition to other networks at points known as switches.

- At the time of the science backbone, the switches for the routing of global Internet communications were situated in the USA. For that reason, at that time intelligence services could intercept a substantial proportion of European Internet communications. Today, only a very small proportion of intra-European Internet communications are routed via the USA.

- A small proportion of intra-European communications are routed via a switch in London to which the British monitoring station GCHQ has access. The majority of communications do not leave the continent: for example, more than 95% of German Internet communications are routed via a switch in Frankfurt.

In practical terms, this means that the ECHELON states have access only to **a very limited proportion** of Internet communications transmitted by cable.

3.3.1.2. Radio communications[1]

The interceptibility of radio communications depends on the range of the electromagnetic waves employed. If the radio waves run along the surface of the earth (so-called **ground waves**), their range is restricted and is determined by the topography of the earth's surface, the degree to which it is built up and the amount of vegetation. If the radio waves are transmitted towards space (so-called **space waves**), two points a substantial distance apart can be linked by means of the reflection of the sky wave from layers of the ionosphere. Multiple reflections substantially increase the range.

The range is determined by the wavelength:

- Very long and long waves (3 kHz – 300 kHz) propagate only via ground waves, because space waves are not reflected. They have very short ranges.

- Medium waves (300 kHz – 3 MHz) propagate via ground waves and at night also via space waves. They are medium-range radio waves.

- Short waves (3 MHz – 30 MHz) propagate primarily via ground waves; multiple reflections make **worldwide** reception possible.

- Ultra-short waves (30 MHz – 300 MHz) propagate only via ground waves, because space waves are not reflected. They propagate in a relatively straight line, like light, with the result that, because of the curvature of the earth, their range is determined by the height of the transmitting and receiving antennae. Depending on power, they have ranges of up to 100 km (roughly 30 km in the case of mobile phones).

- Decimetre and centimetre waves (30 MHz – 30 GHz) propagate in a manner even more akin to light than ultra-short waves. They are easy to focus, clearing the way for low-power, unidirectional transmissions (ground-based microwave radio links). They can only be received by antennae situated almost or exactly in line-of-sight.

Long and medium waves are used only for radio transmitters, radio beacons, etc. Short wave and above all, USW and decimetre/centimetre waves are used for military and civil radio communications.

The details outlined above show that a global communications interception system can only intercept short-wave radio transmissions. In the case of all other types of radio transmission, the interception station must be situated within a 100 km radius (e.g. on a ship, in an embassy).

The practical implication for the ECHELON States is that they can intercept only a very limited proportion of radio communications.

[1] U. Freyer, Message transmission technology, Hanser Verlag, 2000.

3.3.1.3. Communications transmitted by geostationary telecommunications satellites[1]

As already referred to above, decimetre and centimetre waves can very easily be focused to form microwave radio links. If a microwave radio link is set up transmitting to a telecommunications satellite in a high, geostationary orbit and the satellite receives the microwave signals, converts them and transmits them back to earth, large distances can be covered without the use of cables. The range of such a link is essentially restricted only by the fact that the satellite can receive and transmit only in a straight line. For that reason, several satellites are employed to provide worldwide coverage (for more details, see Chapter 4). If ECHELON States operate listening stations in the relevant regions of the earth, in principle they can intercept all telephone, fax and data traffic transmitted via such satellites.

3.3.1.4. Scope for interception from aircraft and ships

It has long been known that special AWACS aircraft are used for the purpose of locating other aircraft over long distances. The radar equipment in these aircraft works in conjunction with a detection system, designed to identify specific objectives, which can locate forms of electronic radiation, classify them and correlate them with radar sightings .They have no separate SIGINT capability[2]. In contrast, the slow-flying EP-3 spy plane used by the US Navy has the capability to intercept microwave, USW and short-wave transmissions. The signals are analysed directly on board and the aircraft is used solely for military purposes[3].

In addition, surface ships, and in coastal regions, submarines are used to intercept military radio transmissions[4].

3.3.1.5. The scope for interception by spy satellites

Provided they are not focused through the use of appropriate antennae, radio waves radiate in all directions, i.e. also into space. Low-orbit Signals Intelligence Satellites can only lock on to the target transmitter for a few minutes in each orbit. In densely populated, highly industrialised areas interception is hampered to such a degree by the high density of transmitters using similar frequencies that it is virtually impossible to filter out individual signals[5]. The satellites cannot be used for the continuous monitoring of civilian radio communications.

Alongside these satellites, the USA operates so-called quasi-geostationary SIGINT satellites stationed in a high earth orbit (42 000 km)[6]. Unlike the geostationary telecommunications satellites, these satellites have an inclination of between 3 and 10°, an apogee of between 39 000 and 42 000 km, and a perigee of between 30 000 and 33 000 km. The satellites are thus not motionless in orbit, but move in a complex elliptical orbit, which enables them to cover a larger area of the earth in the course of one day and to locate sources of radio transmissions. This fact, and the other non-classified characteristics of the satellites, point to their use for purely military purposes.

[1] Hans Dodel, Satellite communications, Hüthig Verlag, 1999.
[2] Letter from the Minister of State in the Federal Defence Ministry, Walter Kolbow, of 14 February 2001.
[3] Süddeutsche Zeitung No 80, 5.4.2001, p. 6.
[4] Jeffrey T. Richelson, The U.S. Intelligence Community, Ballinger, New York, 1989, p. 188, p. 190.
[5] Letter from the Minister of State in the Federal Defence Ministry, Walter Kolbow, of 14 February 2001.
[6] Major Andronov, Zarubezhnoye voyennoye obozreniye, No 12, 1993, p. 37-43.

The signals received are transmitted to the receiving station by means of a strongly-focused, 24 GHz downlink.

3.3.2. Scope for the automatic analysis of intercepted communications: the use of filters

When foreign communications are intercepted, no single telephone connection is monitored on a targeted basis. Instead, some or all of the communications transmitted via the satellite or cable in question are tapped and filtered by computers employing keywords – analysis of every single communication would be completely impossible.

It is easy to filter communications transmitted along a given connection. Specific faxes and e-mails can also be singled out through the use of keywords. If the system has been trained to recognise a particular voice, communications involving that voice can be singled out[1]. However, according to the information available to the rapporteur the automatic recognition of words spoken by any voice is not yet possible. Moreover, the scope for filtering out is restricted by other factors: the ultimate capacity of the computers, the language problem and, above all, the limited number of analysts who can read and assess filtered messages.

When assessing the capabilities of filter systems, consideration must also be given to the fact that in the case of an interception system working on the basis of the 'vacuum-cleaner principle' those technical capabilities are spread across a range of topics. Some of the keywords relate to military security, some to drug trafficking and other forms of international crime, some to the trade in dual-use goods and some to compliance with embargoes. Some of the keywords also relate to economic activities. Any move to narrow down the range of keywords to economically interesting areas would simply run counter to the demands made on intelligence services by governments; what is more, even the end of the Cold War was not enough to prompt such a step[2].

3.3.3. The example of the German Federal Intelligence Service

Department 2 of the German Federal Intelligence Service (FIS) obtains information through the interception of foreign communications. This activity was the subject of a review by the German Federal Constitutional Court. The details made public during the court proceedings[3], combined with the evidence given to the Temporary Committee on 21 November 2000 by Mr Ernst Uhrlau, the coordinator for the secret services in the Federal Chancellor's Office, give an insight into the scope for obtaining intelligence by intercepting satellite communications.

On the basis of their right of access to cable communications or the availability of a greater number of analysts, the capabilities of other intelligence services may be greater in detail terms in given areas. In particular, the monitoring of cable traffic increases the statistical likelihood of success, but not necessarily the number of communications which can be analysed. In fundamental terms, in your rapporteur's view the example of the FIS demonstrates the capabilities and strategies employed by foreign intelligence services in connection with the

[1] Information supplied privately to the rapporteur (confidential source).
[2] Information supplied privately to the rapporteur (confidential source).
[3] BverfG, 1 BvR 2226/94, 14 July 1999, paragraph 1.

monitoring of foreign communications, even if those services do not disclose such matters to the public.

The FIS endeavours, by means of **strategic** telecommunications monitoring, to secure information from foreign countries about foreign countries. With that aim in view, satellite transmissions are intercepted using a series of search terms (which in Germany must be authorised in advance by the so-called G10 Committee[1]). The relevant figures break down as follows (year 2000): of the roughly 10 million international communications routed to and from Germany every day, some 800 000 are transmitted via satellite. Just under 10% of these (75 000) are filtered through a search engine. In your rapporteur's view, this limitation is not imposed by the law (in theoretical terms, and at least prior to the proceedings before the Federal Constitutional Court, a figure of 100% would have been allowable), but derives from technical restrictions, e.g. the limited capacity for analysis.

The number of usable search terms is likewise restricted on technical grounds and by the need to secure authorisation. The grounds for the judgment handed down by the Federal Constitutional Court refer, alongside the purely formal search terms (connections used by foreign nationals or foreign firms abroad), to 2 000 search terms in the sphere of nuclear proliferation, 1 000 in the sphere of the arms trade, 500 in the sphere of terrorism and 400 in the sphere of drug trafficking. However, the procedure has proved relatively unsuccessful in connection with terrorism and drug trafficking.

The search engine checks whether authorised search terms are used in fax and telex communications. Automatic word recognition in voice connections is not yet possible. If the search terms are not found, in technical terms the communications automatically end up in the waste bin; they cannot be analysed, owing to the lack of a legal basis. Every day, five or so communications are logged which are covered by the provisions governing the protection of the German constitution. The monitoring strategy of the FIS is geared to finding clues on which to base further monitoring activities. The monitoring of all foreign communications is not an objective. On the basis of the information available to your rapporteur, this also applies to the SIGINT activities of other foreign intelligence services.

[1] Law on the restriction of the privacy of posts and telecommunications (law on Article 10 of the Basic Law) of 13 August 1968.

4. Satellite communications technology

4.1. The significance of telecommunications satellites

Today, telecommunications satellites form an essential part of the global telecommunications network and have a vital role to play in the provision of television and radio programmes and multimedia services. Nevertheless, the proportion of international communications accounted for by satellite links has decreased substantially over the past few years in Central Europe. In some regions, it has even fallen below 10%[1]. This can be explained by the advantages offered by fibreoptic cables, which can carry a much greater volume of traffic at a higher connection quality.

Today, voice communications are also carried by digital systems. The capacity of digital connections routed via satellites is restricted to **1 890** ISDN-standard (64 kbits/sec) voice channels per transponder on the satellite in question. In contrast, **241 920** voice channels with the same standard can be carried on a single optical fibre. This corresponds to a ratio of **1:128**!

In addition, the quality of connections routed via satellite is lower than those routed via underwater fibreoptic cables. In the case of normal voice transmissions, the loss of quality resulting from the long delay times of several hundred milliseconds is hardly noticeable – although it is perceptible. In the case of data and fax connections, which involve a complicated 'handshaking' procedure, cable offers clear advantages in terms of connection security. At the same time, however, only 15% of the world's population is connected to the global cable network[2].

For certain applications, therefore, satellite systems will continue to offer advantages over cable in the long term. Here are some examples from the civilian sphere:

- National, regional and international telephone and data traffic in areas with a low volume of communications, i.e. in those places where the low rate of use would make a cable connection unprofitable;
- Temporary communications systems used in the context of rescue operations following natural disasters, major events, large-scale building sites, etc.;
- UN missions in regions with an underdeveloped communications infrastructure.
- Flexible/mobile business communications using very small earth stations (VSATs, see below).

This wide range of uses to which satellites are put in the communications sphere can be explained by the following characteristics: the footprint of a single geostationary satellite can cover almost 50% of the earth's surface; impassable regions no longer pose a barrier to communication. In the area concerned, 100% of users are covered, whether on land, at sea or in the air. Satellites can be made operational within a few months, irrespective of the infrastructure available on the spot, they are more reliable than cable and can be replaced more easily.

[1] See the justification for the amendment to the G10 Law in Germany.
[2] Deutsche Telekom homepage: www.detesat.com/deutsch/

The following characteristics of satellite communications must be regarded as drawbacks: the relatively long delay times, the path attenuation, the shorter useful life, by comparison with cable, of 12 to 15 years, the greater vulnerability to damage and the ease of interception.

4.2. How a satellite link operates

As already mentioned (see Chapter 3), by using appropriate antennae microwaves can be very effectively focused, allowing cables to be replaced by microwave radio links. If the transmitting and the receiving antenna are not in line of sight, but rather, as they are on the earth, on the surface of a sphere, then from a given distance onwards the receiving antenna 'disappears' below the horizon owing to the curvature of the earth. The two antennae are thus no longer in line of sight. This would apply, for example, to an intercontinental microwave radio link between Europe and the USA. The antennae would have to be fitted to masts 1.8 km high in order for a link to be established. For this reason, an intercontinental microwave radio link of this kind is simply not feasible, setting aside the issue of the attenuation of the signal by air and water vapour. However, if a kind of mirror for the microwave radio link can be set up in a 'fixed position' high above the earth in space, large distances can be overcome, despite the curvature of the earth, just as a person can see round corners using a traffic mirror. The principle described above is made workable through the use of geostationary satellites.

4.2.1. Geostationary satellites

If a satellite is placed into a circular orbit parallel to the equator in which it circles the earth once every 24 hours, it will follow the rotation of the earth exactly. Looking up from the earth's surface, it seems to stand still at a height of 36 000 km – it has a **geostationary** position. Most communications and television satellites are satellites of this type.

4.2.2. The route followed by signals sent via a satellite communication link

The transmission of signals via satellite can be described as follows:

The signal coming from a cable is transmitted by an earth station equipped with a parabolic antenna to the satellite via an upward microwave radio link, the **uplink**. The satellite receives the signal, regenerates it and transmits it back to another Earth station via a downwards microwave radio link, the **downlink**. From there, the signal is transferred back to a cable network.

In the case of mobile communications, the signal is transmitted directly from the mobile communications unit to the satellite, from where it can be fed into a cable link, via an Earth station, or directly transmitted to a different mobile unit.

4.2.3. The most important satellite communication systems

If necessary, communications coming from **public cable networks** (not necessarily state networks) are transmitted between fixed earth stations, via satellite systems of differing scope, and then fed back into cable networks. A distinction is drawn between the following forms of satellite systems:

- global systems (e.g. INTELSAT)
- regional (continental) systems (e.g. EUTELSAT)

- national systems (e.g. ITALSAT).

Most of these satellites are in a geostationary orbit; 120 private companies throughout the world operate some 1 000 satellites[1].

In addition, the far northern areas of the earth are covered by satellites in a highly eccentric orbit (Russian molnyia orbits) in which the satellites are visible to users in the far north for half their orbit. Two satellites can provide full regional coverage, which is not feasible from a geostationary position above the equator.

Alongside this, the global INMARSAT system – originally established for use at sea – provides a **mobile communications system** by means of which satellite links can be established anywhere in the world. This system also uses geostationary satellites.

The worldwide satellite-based mobile telephone system IRIDIUM, which employed a number of satellites placed at time intervals in low orbits, recently ceased operating on economic grounds (overcapacity).

There is also a rapidly expanding market for so-called VSAT links (VSAT = very small aperture terminal). This involves the use of very small earth stations with antennae with a diameter of between 0.9 and 3.7 metres, which are operated either by firms to meet their own needs (e.g. videoconferences) or by mobile service providers to meet short-term communications requirements (e.g. in connection with meetings). In 1996, 200 000 very small earth stations were in operation around the world. Volkswagen AG operates 3 000 VSAT units, Renault 4 000, General Motors 100 000 and the largest European oil company 12 000. If the client does not arrange for encryption, communication is entirely open[2].

4.2.3.1. Global satellite systems

Through the positioning of satellites above the Atlantic, Indian and Pacific regions, these satellite systems cover the entire globe.

INTELSAT[3]

INTELSAT (International Telecommunications Satellite Organisation) was founded as an authority in 1964 with an organisational structure similar to that of the UN and with the commercial purpose of providing international communications. The members of the organisation were state-owned telecommunications companies. Today, 144 governments are INTELSAT members. In 2001, INTELSAT will be privatised.

INTELSAT now operates a fleet of 19 geostationary satellites, which provide links between more than 200 countries and whose services are rented out to the members of INTELSAT. The members operate their own ground stations. Following the establishment of INTELSAT Business Service (IBS) in 1984, non-members (e.g. telephone companies, large firms, international concerns) can also use the satellites. INTELSAT offers global services such as

[1] G. Thaller, Satellites in Earth Orbit, Franzisverlag, Munich, 1999.
[2] H. Dodel, private information.
[3] INTELSAT homepage:http://www.intelsat.com

communications, television, etc. Telecommunications are transmitted via the C-band and the Ku-band (see below).

INTELSAT satellites are the most important international telecommunications satellites, accounting for a very large proportion of the world market in such communications.

The satellites cover the Atlantic, Indian and Pacific regions (see table, Chapter 5.3).

Ten satellites are positioned above the Atlantic between 304°E and 359°E, the Indian region is covered by six satellites situated between 62°E and 110m.5°E and the Pacific region by three satellites situated between 174°E and 180°E. The high volume of traffic in the Atlantic region is covered by a number of individual satellites positioned at the relevant longitudes.

INTERSPUTNIK[1]

In 1971 the international communications organisation INTERSPUTNIK was founded by nine countries as an agency of the former Soviet Union with a task similar to that of INTELSAT. Today, INTERSPUTNIK is an intergovernmental organisation which the government of any country can join. It now has 24 member countries (including Germany) and some 40 users (including France and England), which are represented by their post offices or national telecommunications companies. Its headquarters are in Moscow.

Telecommunications are transmitted via the C-band and the Ku-band (see below).

Its satellites (Gorizont, Express and Express A, owned by the Russian Federation, and LMI-1, the product of the Lockheed-Martin joint venture) also cover the entire globe: one satellite is positioned above the Atlantic region, with a second planned, three are positioned above the Indian region and two are positioned above the Pacific region (see table, Chapter 5.3).

INMARSAT

Since 1979 INMARSAT (Interim International Maritime Satellite) has provided, by means of its satellite system, worldwide **mobile** communications at sea, in the air and on land and an emergency radio system. INMARSAT was set up as an international organisation at the instigation of the International Maritime Organisation. INMARSAT has since been privatised and has its headquarters in London.

The INMARSAT system consists of nine satellites in geostationary orbits. Four of these satellites – the INMARSAT-III generation – cover the entire globe with the exception of the high polar areas. Each individual satellite covers roughly one-third of the earth's surface. Through their positioning above the four ocean regions (West and East Atlantic, Pacific, Indian Ocean), global coverage is provided. At the same time, each INMARSAT has a number of spot beams which make it possible to focus energy in areas with heavier communications traffic.

Telecommunications are transmitted via the L-band and the Ku-band (see below).

4.2.3.2. Regional satellite systems

[1] INTERSPUTNIK homepage: http://www.intersputnik.com

Individual regions/continents are covered by the footprints of regional satellite systems. As a result, the communications transmitted via them can be received only in those regions.

EUTELSAT[1]

EUTELSAT was founded in 1977 by 17 European postal administrations with the aim of meeting Europe's specific satellite communication requirements and supporting the European space industry. It has its headquarters in Paris and some 40 member countries. EUTELSAT is to be privatised in 2001.

EUTELSAT operates 18 geostationary satellites which cover Europe, Africa and large parts of Asia and establish a link with America. The satellites are positioned between 12.5°W and 48°E. EUTELSAT mainly offers television (850 digital and analog channels) and radio (520 channels) services, but also provides communication links – primarily within Europe, including Russia, e.g. for videoconferences, for the private networks run by large undertakings (including General Motors and Fiat), for press agencies (Reuters, AFP), for providers of financial information and for mobile data transmission services.

Telecommunications are transmitted via the Ku-band.

ARABSAT[2]

ARABSAT is the counterpart to EUTELSAT in the Arab region and was founded in 1976. Membership is made up of 21 Arab countries. ARABSAT satellites are used both for the transmission of television services and for communications.

Telecommunications are transmitted mainly via the C-band.

PALAPA[3]

The Indonesian PALAPA system has been in operation since 1995 and is the south-Asian counterpart to EUTELSAT. Its footprint covers Malaysia, China, Japan, India, Pakistan and other countries in the region.

Telecommunications are transmitted via the C-band and the Ku-band.

4.2.3.3. National satellite systems[4]

Many states meet their own requirements by operating satellite systems with restricted footprints.

One purpose of the French telecommunications satellite **TELECOM** is to link the French departments in Africa and South America with mainland France. Telecommunications are transmitted via the C-band and the Ku-band.

[1] EUTELSAT homepage: http://www.com
[2] ARABSAT homepage: http://www.arabsat.
[3] H.Dodel, Satellite communications, Hüthigverlag, 1999
[4] H.Dodel and Internet research

ITALSAT operates telecommunications satellites which cover the whole of Italy by means of a series of restricted footprints. Reception is therefore possible only in Italy. Telecommunications are transmitted via the Ku-band.

AMOS is an Israeli satellite which primarily offers fixed communication services and whose footprint covers the Middle East. Telecommunications are transmitted via the Ku-band.

The Spanish **HISPASAT** satellites cover Spain and Portugal (KU-spots) and transmit Spanish television programmes to North and South America.

4.2.4. The allocation of frequencies

The International Telecommunications Union is responsible for the allocation of frequencies. For ease of organisation, for radio communication purposes the world has been divided into three regions:

1. Europe, Africa, former Soviet Union, Mongolia
2. North and South America and Greenland
3. Asia, with the exception of countries in region 1, Australia and the South Pacific.

This division, which has become established over the years, was taken over for the purposes of satellite communications and has led to the positioning of large numbers of satellites in certain geostationary areas. The most important frequency bands for satellite communications are:

- the L-band (0.4 – 1.6 GHz) for mobile satellite communications, e.g. via IMMARSAT;
- the C-band (3.6 – 6.6 GHz) for earth stations, e.g. via INTELSAT;
- the Ku-band (10 – 20 GHz) for earth stations, e.g. INTELSAT Ku-spot and EUTELSAT;
- the Ka-band (20 – 46 GHz) for earth stations, e.g. via national satellites such as ITALSAT;
- the V-band (46 – 56 GHz) for very small earth stations (VSATs).

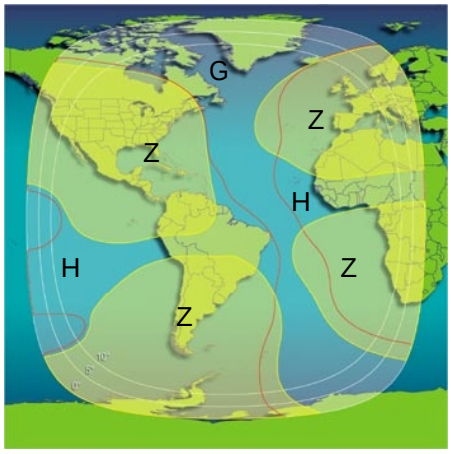
4.2.5. Satellite footprints

The footprint is the area on the earth covered by a satellite antenna. It may embrace up to 50% of the earth's surface, or, by means of signal focusing, be restricted to small, regional spots.

The higher the frequency of the signal emitted, the more it can be focused and the smaller the footprint becomes. The focusing of the satellite signal on smaller footprints can increase the energy of the signal. The smaller the footprint, the stronger the signal, and thus the smaller the receiving antennae may be.

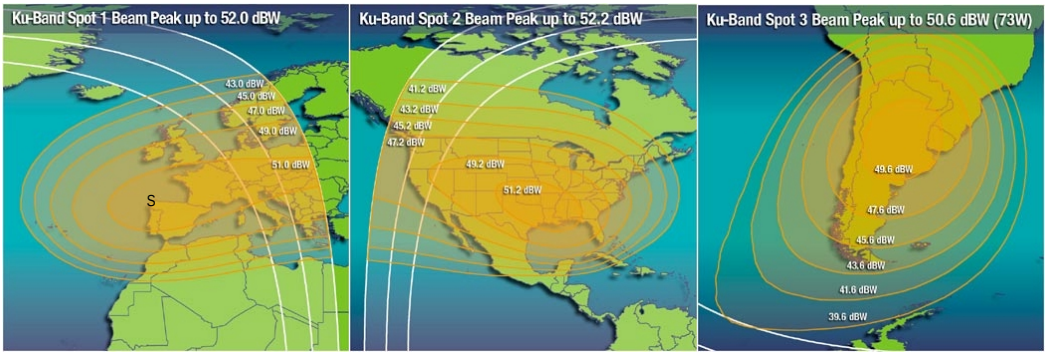
This can briefly be illustrated in greater detail, taking the example of the INTELSAT satellites.

The footprints of the INTELSAT satellites are divided into various beams:



- each satellite's global beam (G) covers roughly one-third of the earth's surface;

- the hemispheric beams (H) each cover an area slightly smaller than half that covered by the global beams. Zone beams (Z) are spots in particular areas of the earth; they are smaller than the hemi-beams. In addition there are so-called spot beams; these are small, precise footprints (see below).



The global, hemispheric and zone beams use C-band frequencies. The spot beams use Ku-band frequencies.

4.2.6. The size of antennae required by an earth station

Parabolic antennae are used as receiving antennae on the earth. The parabolic mirror reflects all incoming waves and focuses them. The actual receiving system is situated in the focal point of the parabolic mirror. The greater the energy of the signal at the receiving point is, the smaller the diameter of the parabolic antenna need be.

The key factor in connection with the investigations conducted for this report is that a proportion of intercontinental communications are transmitted via the C-band in the global beams of the INTELSAT satellites and other satellites (e.g. INTERSPUTNIK) and that satellite dishes with a diameter of roughly 30 m are needed to receive some of these communications (see Chapter 5). Antennae of that size were also needed for the first stations set up to intercept satellite communications, since the first generation of INTELSAT satellites had only global beams and signal transmission technology was much less sophisticated than it is today. These dishes, some of which have a diameter of more than 30 m, are still used at the stations in question, even though they are no longer required on purely technical grounds.

Today, the typical antennae required for INTELSAT communications in the C-band have a diameter of between 13 and 18 m. In some individual cases, e.g. INTELSAT 511, a larger antenna is required for the global beam. In the case of the newest INTELSAT satellites, antennae with a diameter of up to 5 m are sufficient for the zone beams in the C-band.

Antennae with a diameter of between 2 and 25 m are required to receive C-band communications from INTERSPUTNIK.

Antennae with a diameter of between 2 and 10 m are required for the Ku-spots of the INTELSAT satellites and other satellites (EUTELSAT Ku-band, AMOS Ku-band, etc.).

In the case of very small earth stations, which operate in the V-band and whose signal, by virtue of the high frequency, can be focused even more strongly than those in the Ku-band, antennae with a diameter of between 0.9 and 3.7 m are adequate (e.g. VSATs from EUTELSAT or INMARSAT).

5. Clues to the existence of at least one global interception system

5.1. Why is it necessary to work on the basis of clues?

It is only natural that secret services do not disclose details of their work. Consequently there is, at least officially, no statement by the foreign intelligence services of the ECHELON states that they work together to operate a global interception system. The existence of such a system thus needs to be proved by gathering as many clues as possible, thereby building up a convincing body of evidence.

The trail of clues which constitutes evidence of this kind is made up of three elements:

- evidence that the foreign intelligence services in the ECHELON states intercept private and business communications;
- evidence that interception stations operated by the ECHELON states are to be found in the parts of the world where they would be needed in the light of the technical requirements of the civilian satellite communication system;
- evidence that there is a closer than usual association between the intelligence services of these states. For the purposes of proving the existence of such an association, it is irrelevant whether this extends to the acceptance from partners of applications for the interception of messages which are then forwarded to them in the form of unevaluated raw material. This question is only relevant when investigating the hierarchies within such an interception association.

5.1.1. Evidence of interception activity on the part of foreign intelligence services

At least in democracies, intelligence services work on the basis of laws which define their purpose and/or powers. It is thus easy to prove that in many of these countries foreign intelligence services exist which intercept civilian communications. This is true of the five "ECHELON" states, which all operate such services. There is no need for specific additional proof that any of these states intercept communications entering and leaving their territory. Satellite communications also permit some intelligence communications intended for recipients abroad to be intercepted from the country's own territory. In none of the five ECHELON states is there any legal impediment to intelligence services doing this. The logic underlying the method for the strategic monitoring of foreign communications, and its at least partly overtly acknowledged purpose, make it practically certain that the intelligence services do in fact use it to that end.[1]

5.1.2. Evidence for the existence of stations in the necessary geographical areas

The only restriction on the attempt to build up worldwide monitoring of satellite communications arises from the technical constraints imposed by these communications themselves. There is no place from which **all** satellite communications can be intercepted (see point 4).

[1] Your rapporteur has evidence that this is the case. Source protected.

It would be possible for a worldwide interception system to be constructed, subject to three conditions:

- the operator has national territory of its own in all the necessary parts of the world;
- the operator has, in all the necessary parts of the world, either national territory of its own or a right of access entitling it to operate or share the use of stations;
- the operator is a group of states which has formed an intelligence association and operates the system in the necessary parts of the world.

None of the ECHELON states would be able to operate a global system on its own. The USA has, at least formally, no colonies. Canada, Australia and New Zealand also have no territory outside the narrower confines of their countries, and the UK would also not be able to operate a global interception system on its own (see Chapter 6).

5.1.3. Evidence of a close intelligence association

On the other hand it has not been disclosed whether and to what extent the ECHELON states cooperate with one another in the intelligence field. Normally cooperation between intelligence services takes place bilaterally and on the basis of an exchange of evaluated material. A multilateral union is in itself something very unusual; if one adds to this the regular exchange of raw material, this would be a qualitatively new form of cooperation. The existence of such an association can only be proved on the basis of clues.

5.2. How can a satellite communications interception station be recognised?

5.2.1. Criterion 1: Accessibility of the installation

Installations with large antennae belonging to the post office, broadcasters or research institutions are accessible to visitors, at least by appointment; interception stations are not. They are generally operated, at least, in name, by the military, which also carries out the technical work of interception. For the NSA, for example, the stations are operated by the Naval Security Group (NAVSECGRU) or the Air Intelligence Agency (AIA). In the British stations, the RAF operates the installations for the British GCHQ intelligence service. This arrangement enables the installations to be guarded with military efficiency and at the same time serves as cover.

5.2.2. Criterion 2: Type of antenna

Various types of antennae are used in the installations which fulfil criterion 1, each with a different characteristic shape, which provides evidence as to the purpose of the interception station. Arrangements of tall rod antennae in a large-diameter circle (Wullenweber antennae), for example, are used for locating the direction of radio signals. Similarly, circular arrangements of rhombic-shaped antennae (Pusher antennae) serve the same purpose. Omnidirectional antennae, which look like giant conventional TV antennae, are used to intercept non-directional radio signals. **To receive satellite signals, however, only parabolic antennae are used.** If the parabolic antennae are standing on an open site, it is possible to calculate on the basis of their position, their elevation and their compass (azimuth) angle which satellite is being received. This is possible, for example, in Morwenstow (UK), Yakima (USA) or Sugar Grove (USA).

However, most often parabolic antennae are concealed under spherical white covers known as radomes: these protect the antennae, but also conceal which direction they are pointing in.

If parabolic antennae or radomes are positioned on an intercepting station site, one may be certain that they are receiving signals from satellites, though this does not prove what type of signals these are.

5.2.3. Criterion 3: Size of antenna

Satellite receiving antennae on a site which meets criterion 1 may be intended for various purposes:

- receiving station for military communications;
- receiving station for spy satellites (pictures, radar);
- receiving station for military SIGINT satellites;
- receiving station for interception of civilian communications satellites.

It is not possible to tell from outside what function these antennae or radomes serve. However, there are minimum sizes, dictated by technical requirements, for antennae intended to receive the 'global beam' in the C-band of satellite-based civilian international communications. The first generation of these satellites needed antennae with a diameter of 25-30 m; nowadays 15-18 m is enough. The automatic computer filtering of signals received calls for the highest possible signal quality, so for intelligence purposes an antenna at the upper end of the scale is chosen. Because the antennae are mounted on stands, the diameter of the radomes is even greater than the diameter of the antennae.

5.2.4 Conclusion

As far as your rapporteur knows there is no military application for antennae of this size. Consequently, if they are found on a site meeting criterion 1, it may be concluded that civilian satellite communications are being intercepted on that site.

5.3. Publicly accessible data about known interception stations

5.3.1. Method

With a view to determining which stations meet the criteria set out in Chapter 5.2. and thus form part of the global interception system and establishing what tasks they have, the relevant, somewhat contradictory, literature (Hager[1], Richelson[2], Campbell[3]) declassified documents[1], the

[1] Hager, Nicky: EXPOSING THE GLOBAL SURVEILLANCE SYSTEM http://www.ncoic.com/echelon1.htm
Hager, Nicky: Secret Power. New Zealand's Role in the international Spy Network, New Zealand 1996.
[2] Richelson, Jeffrey, Desperately seeking Signals, 4 2000, the Bulletin of the Atomic Scientists, http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html
Richelson, T. Jeffrey, The U.S. Intelligence Community, Westview Press 1999.
[3] Campbell, Duncan, Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5, 10 1999, STOA, http://www.europarl.eu.int/dg4/stoa/en/publi/pdf/98-14-01-2en.pdf
Campbell, Duncan: Inside Echelon, 25.7.2000http://www.heise.de/tp/deutsch/special/ech/6928/1.html
Campbell, Duncan: Interception Capabilities n- Impact and Exploitation – Echelon and its role in COMINT, submitted to the Temporary Committee on 22 January 2001
Federation of American Scientists, http://www.fas.org/irp/nsa/nsafacil.html

homepage of the Federation of American Scientists[2] and operators' homepages[3] (NSA, AIA, etc.) and other Internet publications were analysed. In addition, the footprints of telecommunications satellites were collated, the requisite antenna sizes were calculated and these footprints and antenna locations were entered, along with the locations of possible stations, on world maps.

5.3.2. Detailed analysis

The following principles relating to the physics of satellite communications apply in connection with the analysis (see also Chapter 4):

- A satellite antenna can only record communications transmitted within the footprint in which it is located. In order to receive communications, which are mainly transmitted in the C-band and Ku-band, an antenna must lie within the footprints containing those bands.
- A satellite antenna is required for each separate global beam, even if beams from two satellites overlap.
- If a satellite has other footprints in addition to the global beam, which is typical of today's generations of satellites, a single satellite antenna can no longer record all the communications transmitted via that satellite, since a single satellite antenna cannot be located in every one of the satellite's footprints. In order to capture a satellite's hemispheric beam and its global beam, therefore, two satellite antennae are required in different areas (see illustration of the footprints in Chapter 4). If further beams (zone and spot beams) are involved, further satellite antennae are required. However, different, overlapping beams from a single satellite can be captured by one satellite antenna, since it is technically feasible to separate different frequency bands when reception takes place.

In addition, the requirements referred to in Chapter 5.2. apply: the non-accessibility of the installations, on the grounds that they are operated by the military[4], the fact that parabolic antennae are required to receive satellite signals and the fact that the size of the satellite antennae needed to capture the C-band in the global beam is more than 25 m for the first INTELSAT generation and more than 15 to 18 m for later generations.

5.3.2.1. The parallel between the development of INTELSAT and the building of stations

A global interception system must grow as communications develop. Accordingly, the start of the satellite communications era must lead to the establishment of stations and the introduction of new generations of satellites must lead to the establishment of new stations and the building of new satellite antennae which can cope with the new technical requirements. The number of stations and the number of satellite antennae must increase whenever this is necessary in order to cover the full volume of communications traffic.

If we turn this equation round, it is no coincidence that, when new footprints come into being, new stations are established and new satellite antennae are built. Instead, this can be seen as a clue to the existence of a communications interception station.

Since the INTELSAT satellites were the first telecommunications satellites, and, moreover, the

---

[1] Richelson, Jeffrey: Newly released documents on the restrictions NSA places on reporting the identities of US-persons: Declassified: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html

[2] Federation of American Scientists.

[3] Military.com; *.mil-Homepages.

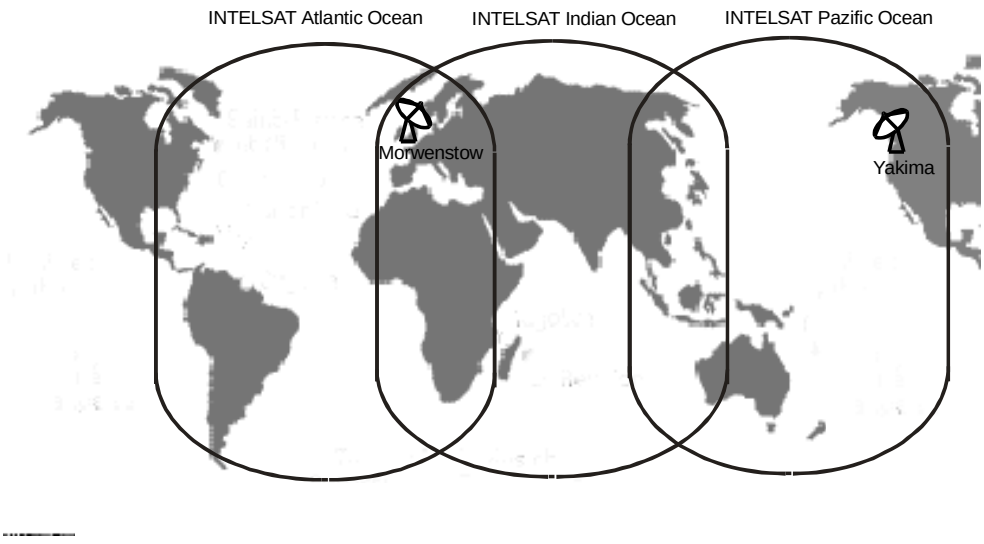
[4] Abbreviations used: NAVSECGRU: Naval Security Group, INSCOM: United States Army Intelligence And Security Command, AIA: Air Intelligence Agency, IG: Intelligence Group, IS: Intelligence Squadron, IW: Intelligence Wing, IOG: Information Operation Group, MIG: Military Intelligence Group.

first to cover the entire globe, it is only logical that the introduction of the new generations of INTELSAT satellites should go hand-in-hand with the establishment of new and bigger stations.

The first generation

As long ago as 1965 the first INTELSAT satellite (Early Bird) was placed in a geostationary orbit. Its transmission capacity was still low and its footprint covered only the northern hemisphere.
When the second and third INTELSAT generations came into operation, in 1967 and 1968 respectively, global coverage was achieved for the first time. The satellites' global beams covered the Atlantic, Pacific and Indian Ocean areas. Satellite systems with smaller footprints had not yet been introduced. Three satellite antennae were thus needed in order to record all communications. Since two of the global beams overlapped over the European continent, in that area the global footprints of two satellites could be covered by two satellite antennae trained in different directions.

First generation of INTELSAT satellites providing global coverage



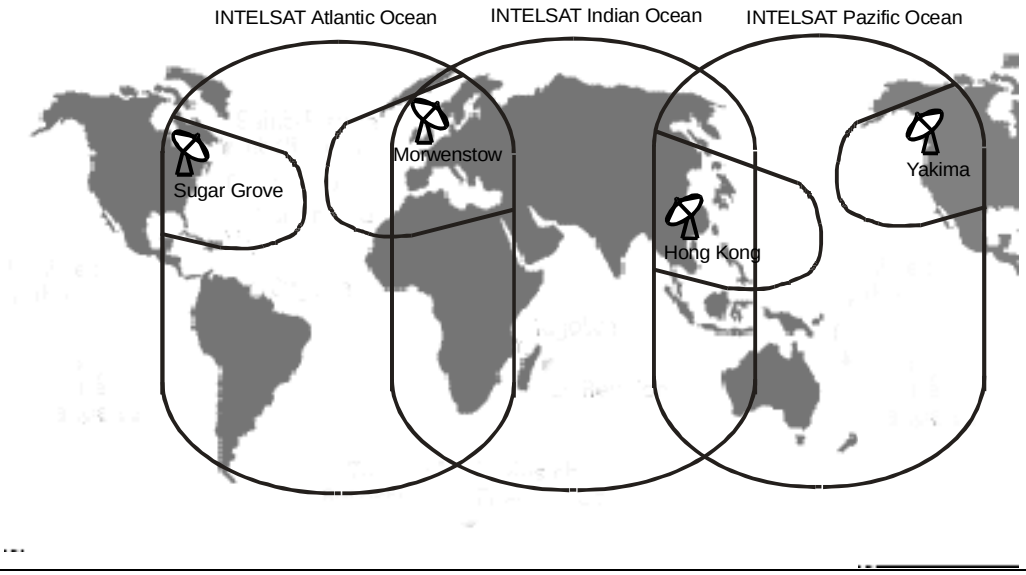
In 1970 the **Yakima** station was established in the north-western USA and in 1972/73 the **Morwenstow** station was built in southern England. At that time, Yakima had one large antenna (trained towards the Pacific) and Morwenstow had two large antennae (one trained towards the Atlantic, the other towards the Indian Ocean). By virtue of the location of the two stations, all communications could be recorded. In addition, in 1974 the first large satellite antenna was built in Menwith Hill.

The second global generation

The second generation of INTELSAT satellites (IV and IVA) were developed in the 1970s and placed in a geostationary orbit (1971 and 1975). The new satellites, which also provided global coverage and had a much larger number of communications channels (4000-6000), used, in addition to the global beams, zone beams in the northern hemisphere (see Chapter 4). One zone

beam covered the eastern USA, a second the western USA, a third western Europe and a fourth east Asia. As a result, it was no longer possible to record all communications using two stations equipped with three satellite antennae. Using the existing stations in Yakima, the zone beam in the western USA could be covered; Morwenstow covered the zone beam over Europe. A station in the eastern USA and another in east Asia were needed in order to cover the other two zone beams.

Second generation of INTELSAT satellites providing global coverage



In the late 1970s the **Sugar Grove** station in the eastern USA was developed (the station already existed for the purpose of intercepting Russian communications); it came into operation in 1980. A station in **Hong Kong** was also set up in the late 1970s.
As a result, in the 1980s global interception of INTELSAT communications was possible using the four stations - Yakima, Morwenstow, Sugar Grove and Hong Kong.

The later INTELSAT satellites, which used zone beams and spot beams in addition to the global and hemispheric beams, made further stations in various parts of the world necessary. Here it is very difficult to establish a link with the development of further stations and/or the introduction of new satellite antennae.

Since, in addition, it is difficult to gain access to information about stations, it cannot be determined with any certainty which satellites using which beams are covered by which stations. However, the footprints in which known stations are located can be determined.

5.3.2.2. Global coverage by means of stations which are known to intercept transmissions from telecommunications satellites

Today, global satellite communications are provided by satellites operated by INTELSAT, INMARSAT and INTERSPUTNIK. The division of the earth into three footprints (Indian Ocean, Pacific and Atlantic areas), introduced when the first generations of satellites were sent into space, has been retained. In each of the footprints there are stations which meet the criteria

which characterise them as interception stations:

Satellites over the Indian Ocean:

INTELSAT 604 (60°E), 602 (62°E), 804 (64°E), 704 (66°E) EXPRESS 6A (80°E) INMARSAT Indian Ocean area	Geraldton, Australia Pine Gap, Australia Morwenstow, England Menwith Hill, England
INTELSAT APR1 (83°), APR-2 (110,5°)	Geraldton, Australia Pine Gap, Australia Misawa, Japan

Satellites over the Pacific:

INTELSAT 802 (174°), 702 (176°), 701 (180°) GORIZONT 41 (130°E), 42 (142°E), LM-1 (75°E) INMARSAT Pacific area	Waihopai, New Zealand Geraldton, Australia Pine Gap, Australia Misawa, Japan Yakima, USA - only Intelsat and Inmarsat

Satellites over the Atlantic:

INTELSAT 805 (304,5°), 706 (307°), 709 (310°) 601 (325,5°), 801 (328°), 511(330,5°), 605 (332,5°), 603 (335,5°), 705 (342°) EXPRESS 2 (14°W), 3A (11°W) INMARSAT Atlantic area	Sugar Grove, USA Buckley Field, USA Sabana Seca, Puerto Rico Morwenstow, England Menwith Hill, England
INTELSAT 707 (359°)	Morwenstow, England Menwith Hill, England

This shows that the global interception of communications is feasible.

In addition, there are further stations which, although they do not meet the criterion of antenna size, may still form part of the global interception system. These stations could be used to cover the zone or spot beams of satellites whose global beams are intercepted by other stations or for whose global beam no large satellite antennae are required.

5.3.2.3. The stations in detail

In the detailed descriptions of the stations a distinction is drawn between stations which are clearly used to intercept transmissions from telecommunications satellites (criteria outlined in Chapter 5.2.) and stations whose role cannot be proven with the aid of those criteria.

5.3.2.3.1. Stations used to intercept transmissions from telecommunications satellites

The following stations meet the criteria outlined in Chapter 5.2., criteria which point to a role in intercepting transmissions from telecommunications satellites:

Yakima, USA (120°W, 46°N)
The station was established in 1970, at the same time as the first generation of satellites were put into orbit. Since 1995, the Air Intelligence Agency (AIA), 544th Intelligence Group (Detachment 4), has been stationed in Yakima, along with the Naval Security Group (NAVSECGRU). Six satellite antennae have been installed on the site; the sources give no clue as to the size of the antennae. Hager describes the antennae as large and claims that they are trained on INTELSAT satellites over the Pacific (two satellite antennae) and INTELSAT satellites over the Atlantic, and on INMARSAT Satellite 2.
The fact that Yakima was established at the same time as the first generation of INTELSAT satellites went into orbit, and the general description of the tasks of the 544th Intelligence Group, suggest that the station has a role in global communications surveillance. A further clue is provided by Yakima's proximity to a satellite receiving station, which lies 100 miles to the north.

Sugar Grove, USA (80°W, 39°N)
Sugar Grove was established at the same time as the second generation of INTELSAT satellites came into operation, in the late 1970s. The NAVSECGRU and the AIA, 544th Intelligence Group (Detachment 3), are stationed at Sugar Grove. According to information provided by a variety of authors, the station has 10 satellite antennae, three of which have a diameter larger than 18 m (18.2 m, 32.3 m and 46 m) and which are thus clearly used to intercept transmissions from telecommunications satellites. One of the tasks performed at the station by Detachment 3 of the 544th IG is to provide intelligence support for the collection by Navy field stations of information transmitted by telecommunications satellites[1].
In addition, Sugar Grove is situated close (60 miles) to the Etam satellite receiving station.

Sabana Seca, Puerto Rico (66°W, 18°N)
NAVSECGRU was first stationed in Sabana Seca in 1952. In 1995, it was joined by the AIA, 544th IG (Detachment 2). The station has at least one satellite antenna with a diameter of 32 m and four further small satellite antennae.
According to official information, the station's tasks are to perform 'satellite communication processing', to provide 'cryptologic and communications service' and to support Navy and DoD operations, including the collection of COMSAT information (from a description of the 544th IG). In future, Sabana Seca is set to become the first field station for the analysis and processing of satellite communications.

Morwenstow, England (4°W, 51°N)
Like Yakima, Morwenstow was established in the early 1970s, at the same time as the first generation of INTELSAT satellites went into space. Morwenstow is operated by the British Intelligence Service (GCHQ). The Morwenstow site houses some 30 satellite antennae, two of which have a diameter of 30 m; no details are available of the size of the other antennae.
No official information has been issued regarding the station's role; however, the size and number of the satellite antennae and the location of the station, only 110 km from the telecommunications station in Goonhilly, leave no doubt as to its task of intercepting transmissions from telecommunications satellites.

[1] 'It provides enhanced intelligence support to Air Force operational commanders and other consumers of communications satellite information collected by Navy-commanded field stations.' from the home page of the 544th Intelligence Group http://www.aia.af.mil

Menwith Hill, England (2°W, 53°N)
Menwith Hill was established in 1956 and by 1974 already housed eight satellite antennae. Today, the figure is roughly 30, some of which have a diameter of more than 20 m. The British and Americans work together at Menwith Hill. The American services stationed there are NAVSECGRU, the AIA (451st IOS) and INSCOM, which has command of the station. The land on which Menwith Hill stands belongs to the UK Defence Ministry and is rented to the US Administration. According to official information, Menwith Hill's role is 'to provide rapid radio relay and to conduct communications research'. According to statement by Richelson and the Federation of American Scientists, Menwith Hill is both an earth station for spy satellites and an earth station for the interception of transmissions from Russian telecommunications satellites.

Geraldton, Australia (114°O, 28°S)
The station was established in the early 1990s. It is run by the Australian Secret Service (DSD), and it is partly manned by British servicemen previously stationed in Hong Kong (see above). According to Hager, six satellite antennae, at least one of which has a diameter of roughly 20 m (estimate), are trained on satellites above the Indian Ocean and the Pacific.
According to statements made under oath in the Australian Parliament by an expert, transmission from telecommunications satellites are intercepted at Geraldton[1].

Pine Gap, Australia (133°O, 23°S)
The station in Pine Gap was established in 1966. It is run by the Australian Secret Service (DSD), and roughly half of the 900 station personnel are Americans from the CIA and NAVSECGRU[2].
Pine Gap has 18 satellite antennae, one with a diameter of roughly 30 m and another with a diameter of roughly 20 m. According to official sources, and information provided by various authors, since its inception Pine Gap has been an earth station for SIGINT satellites. Station personnel control and guide various spy satellites and receive, process and analyse their signals. The large satellite antennae also suggest that transmissions from telecommunications satellites are intercepted, since no such antennae are required for work with SIGINT satellites. Until 1980 no Australians were allowed to work in the signals analysis department; since then, they have been granted free access to all parts of the station, with the exception of the Americans' own cryptography room.

Misawa, Japan (141°O, 40°N)
The station in Misawa was established in 1948 and is manned by Japanese and Americans. The American services represented are NAVSECGRU, INSCOM and some AIA groups (544th IG, 301st IS). The site houses around 14 satellite antennae, some of which have a diameter of roughly 20 m (estimate). Officially, Misawa acts as a 'cryptology operations centre'. According to information supplied by Richelson, the station is used to intercept transmissions from the Russian Molnyia satellites and other Russian telecommunications satellites.

Waihopai, New Zealand (173°O, 41°S)
Waihopai was established in 1989. It started with one large antenna, with a diameter of 18 m, and two smaller antennae were added later. According to Hager, the large antenna is trained on

[1] Proof Committee Hansard, Joint Standing Committee on Treaties, Reference: Pine Gap, 9 August 1999, Canberra; http://www.aph.gov.au/hansard
[2] Proof Committee Hansard, Joint Standing Committee on Treaties, Reference: Pine Gap, 9 August 1999, Canberra; http://www.aph.gov.au/hansard

INTELSAT 701 in orbit above the Pacific.

Buckley Field, Denver, Colorado, USA (104°W, 40°N)
The station was established in 1972 and is home to the 544th IG (Detachment 45). The site houses some five satellite antennae, four of which have a diameter of roughly 20 m. The station's official task is to collect, process and analyse data about nuclear events obtained by SIGINT satellites. The size of the satellite antennae points to a role in intercepting civilian communications.

Hong Kong (22°N, 114°O)
The station was established in the late 1970s, at the same time as the second generation of INTELSAT satellites were put in space, and was equipped with large satellite antennae. No details are available of the exact sizes. In 1994, a start was made on the decommissioning of the station; the antennae were taken to Australia. It is not clear which station (Geraldton, Pine Gap or Misawa, Japan) has taken over the Hong Kong station's tasks, which may have been divided among several stations.

5.3.2.3.2. Further stations

The roles of the following stations cannot be clearly established on the basis of the criteria referred to above:

Leitrim, Canada (75°W, 45°N)
Leitrim is part of an exchange programme between Canadian and America military units. According to the Navy, therefore, some 30 persons are stationed in Leitrim. In 1985 the first of four satellite antennae was installed, of which the two larger have a diameter of no more than roughly 12 m (estimate). According to official information, the station's task is to provide 'cryptologic rating' and to intercept diplomatic communications.

Bad Aibling, Germany (12°O, 47°N)
The station near Bad Aibling, at which roughly 750 Americans work, was taken over by the US Army in 1952 (from 1972 to 1994 it was in the hands of the Department of Defense). NAVSECGRU, INSCOM (66th IG, 718th IG) and various AIA groups (402nd IG, 26th IOG) are stationed in Bad Aibling. The station has 14 satellite antennae, none of which has a diameter of more than 18 m. According to official information, Bad Aibling has the following tasks: 'Rapid Radio Relay and Secure Commo, Support to DoD and Unified Commands, Medium and Longhand Commo HF& Satellite, Communication Physics Research, Test and Evaluate Commo Equipment'. According to Richelson, Bad Aibling is an earth station for SIGINT satellites and for the interception of transmissions from Russian telecommunications satellites.

Ayios Nikolaos, Cyprus (32°O, 35°N)
Ayios Nilolaos on Cyprus is a British station. The station, which has nine satellite antennae whose size is unknown, is manned by two units, the 'Signals Regiment Radio and the Signals Unit (RAF)'.
The station's location, close to the Arab states, and the fact that Ayios Nikolaos is the only station sited within certain footprints (above all spot beams) in this area, point to its having an important role in intelligence gathering.

Shoal Bay, Australia (134°O, 13°S)
Shoal Bay is a station run solely by the Australian Intelligence Service. The station reportedly has 10 satellite antennae; no official information is available regarding their size. Of the satellite antennae visible on photographs, the five larger ones have a maximum diameter of 8 m, and the sixth antenna visible is smaller still. According to information provided by Richelson, the antennae are trained on the Indonesian PALAPA satellites. It is not clear whether the station is part of the global system for the interception of civilian communications.

Guam, Pacific (144°O, 13°S)
Guam was established in 1898. It now houses a Naval Computer and Telecommunications Station manned by the 544th IG of the AIA and Navy soldiers. The station has at least two satellite antennae whose size is unknown. The station's role is thus not clear.

Kunia, Hawaii (158°W, 21°N)
This station has been operated by NAVSECGRU and the AIA since 1993 as a Regional Security Operations Centre (RSOC). Its tasks include the provision of information and communications and cryptological support. Its broader role is not clear.

Medina Annex, Texas, USA (98°W, 29°N)
Like Kunia, Medina, which was established in 1993, is a RSOC operated by NAVSECGRU and AIA units with tasks in the Caribbean.

Fort Gordon (81°W, 31°N)
Fort Gordon is also an RSOC, operated by INSCOM and the AIA (702nd IG, 721st IB, 202nd IB, 31st IS), whose tasks are unclear.

Fort Mead, USA (76°W, 39°N)
Ford Mead is the headquarters of the NSA.

5.3.3. Summary of the findings

The following conclusions can be drawn from the information collected concerning the stations and satellites and from the requirements outlined above:
1. In each footprint there are interception stations which cover at least some of the global beams and are equipped with at least one antenna with a diameter greater than 18 m. They are stations which are operated by the Americans or British or where American or British servicemen carry out intelligence activities. This is convincing evidence for the existence of a global interception system.
2. The expansion of INTELSAT communications and the establishment, at the same time, of the corresponding interception stations show that the system is intended to provide global coverage.
3. On the basis of points 1 and 2, certain stations can clearly be identified as stations which intercept international satellite communications.
4. The information regarding stations contained in the declassified documents and issued by the operators (AIA, NSA, Navy, etc.) can be regarded as proof of the existence and activities of the stations concerned.
5. Some stations are located in the areas covered by the beams or spots of several satellites, so that a large proportion of the relevant communications can be intercepted.

6. There are some other stations which, although they have no large antennae, may also be part of the system, since they can receive communications from the beams and spots. In this case, evidence other than the size of the antennae must be adduced.
7. Some of the stations are situated in immediate proximity to normal earth stations for telecommunications satellites.

5.4. The UKUSA Agreement

A SIGINT agreement signed in 1948 between the United Kingdom, the United States and Australia, Canada and New Zealand is referred to as the UKUSA Agreement.

5.4.1. The historical development of the UKUSA Agreement[1]

The UKUSA Agreement represents a continuation of the cooperation between the USA and the UK which dates back to the First World War and which became very close during the Second World War.
It was the Americans who instigated the establishment of a SIGINT alliance at a meeting with the British in London in August 1940[2]. In February 1941, American cryptoanalysts delivered a cipher machine (PURPLE) to the United Kingdom. Cooperation in the sphere of cryptoanalysis began in spring 1941[3]. Intelligence cooperation was stepped up in response to the joint fleet operations in the North Atlantic in summer 1941. In June 1941 the British broke the German fleet code, ENIGMA.

America's entry into the war led to SIGINT cooperation being stepped up. In 1942, American cryptoanalysts from the Naval SIGINT Agency began work in the United Kingdom[4]. Liaison between the submarine tracking rooms in London, Washington and, from May 1943 onwards, Ottawa in Canada was so close that, according to a statement by one individual involved at the time, they worked like a single organisation[5].
In spring 1943 the BRUSA-SIGINT Agreement was signed, and personnel were exchanged. The agreement primarily concerns the division of work and its main substance is summarised in the first three paragraphs: they cover the exchange of all information obtained by means of the discovery, identification and interception of signals and the cracking of codes and encryption processes. The Americans were primarily responsible for Japan, the British for Germany and Italy[6].

---

[1] Christopher Andrew, "The making of the Anglo-American SIGINT Alliance" in E. Hayden, h. Peake and S. Halpern eds, In the Name of Intelligence. Essays in honor of Washington Pforzheimer (Washington NIBC Press 1995) pp. 95-109.
[2] ibidem, p. 99: 'At a meeting in London on 31 August 1940 between the British Chiefs of Staff and the American Military Observer Mission, the US Army representative, Brigadier General George V. Strong, reported that "it had recently been arranged in principle between the British and the United States Governments that periodic exchange of information would be desirable," and said that "the time had come or a free exchange of intelligence". (COS (40)289, CAB 79/6, PRO. Smith, The Ultra Magic Deals, pp. 38, 43-4. Sir F.H. Hinsley, et al., British Intelligence in the Second World War, vol.I, pp.312-13).
[3] Ibidem, p. 100: ' In the spring of 1941, Steward Menzies, the Chief of SIS, appointed an SIS liaison officer to the British Joint Services Mission in Washington, Tim O´Connor, …, to advice him on cryptologic collaboration'.
[4] Ibidem, p. 100 (Sir F.H. Hinsley, et al., British Intelligence in the Second World War, vol. II, p. 56)
[5] Ibidem, p. 101 (Sir F.H. Hinsley, et al., British Intelligence in the Second World War, vol. II, p. 48)
[6] Ibidem, p.101-2: Interviews with Sir F.H. Hinsley, 'Operations of the Military Intelligence Service War Department London (MIS WD London),' 11 June 1945, Tab A, RG 457 SRH-110, NAW

Following the war, the UK was the prime mover behind the continuation of a SIGINT alliance. The foundations were laid in the course of a world tour undertaken in spring 1945 by British intelligence agents (including Sir Harry Hinsley, whose books are used as source material in the articles quoted in the footnotes). One aim was to transfer SIGINT personnel from Europe to the Pacific to take part in the war against Japan. In that connection, an agreement was reached to provide the Australian intelligence services with resources and personnel (British). The intelligence agents returned to the USA via New Zealand and Canada.
In September 1945 Truman signed a top-secret memorandum whose provisions formed the cornerstone of a peacetime SIGINT alliance[1]. Immediately thereafter, negotiations on an agreement opened between the British and Americans. In addition, a British delegation made contact with the Canadian and Australians with a view to discussing their involvement. In February and March 1946 a top-secret Anglo-American SIGINT conference took place at which the details of an alliance were discussed. The British were authorised by the Canadians and Australians to act on their behalf. The conference produced what was still a classified agreement, running to some 25 pages, which laid down the detailed arrangements for a SIGINT agreement between the United States and the British Commonwealth. Further discussions took place during the two following years, culminating in the signing of the definitive text of the UKUSA Agreement in June 1948[2].

5.4.2. Evidence for the existence of the agreement

Thus far, the signatory states have not officially acknowledged the existence of the UKUSA Agreement. Nevertheless, various pieces of evidence point clearly to the fact that it does indeed exist.

5.4.2.1. The Navy acronym list

According to the US Navy[3], UKUSA stands for 'United Kingdom-USA' and refers to a '5-nation SIGINT agreement'.

5.4.2.2. Statement by the Head of the DSD

The Head of the Australian Intelligence Service (DSD) confirmed the existence of the agreement in an interview: according to the information he gave, the Australian Secret Service cooperates with other overseas intelligence agencies under the UKUSA Agreement[4].

---

[1] Truman, Memorandum for the Secretaries of the State, War and the Navy, 12 Sept. 1945: 'The Secretary of War and the Secretary of the Navy are hereby authorised to direct the Chief of Staff, U.S. Army and the Commander in Chief, U.S. Fleet; and Chief of Naval Operations to continue collaboration in the field of communication intelligence between the United States Army and Navy and the British, and to extend, modify or discontinue this collaboration, as determined to be in the best interests of the United States.' (from Bradley F. Smith, The Ultra-Magic Deals and the Most Secret Special Relationship (Novato, Ca: Presidio 1993))

[2] Christopher Andrew, 'he making of the Anglo-American SIGINT Alliance' in E. Hayden, h. Peake and S. Halpern eds, In the Name of Intelligence. Essays in honor of Washington Pforzheimer (Washington NIBC Press 1995) pp. 95 –109: Interviews with Sir Harry Hinsley, March/April 1994, who did a part of the negotiations; Interviews with Dr. Louis Tordella, Deputy Director of NSA from 1958 to 1974, who was present at the signing.

[3] 'Terms/Abbreviations/Acronyms' published by the US Navy and Marine Corps Intelligence Training Centre (NMITC) at http://www.cnet.navy.mil/nmitc/training/u.html

[4] Martin Brady, Head of the DSD, Canberra 16 March 2000.

5.4.2.3. Report by the Canadian Parliamentary Security and Intelligence Committee

This report describes how Canada cooperates with some of its closest and longest-standing allies in the intelligence sphere. The report names the allies concerned: the United States (NSA), the United Kingdom (GCHQ), Australia (DSD) and New Zealand (GCSB). The report does not name the agreement.

5.4.2.4. Statement by the former Deputy Director of the NSA, Dr Louis Torella

In an interview with Christopher Andrew, a professor at Cambridge University, conducted in November 1987 and April 1992, the former Deputy Director of the NSA, Dr Louis Torella, who was present when the agreement was signed, confirmed that it does exist[1].

5.4.2.5. Letter from the former Head of HCHQ, Joe Hooper

The former Head of GCHQ, Joe Hooper, refers to the UKUSA Agreement in a letter to the former Director of the NSA, Marshall S. Carter.

5.4.2.6. Rapporteur's discussion partners

Your rapporteur has spoken about the agreement with several persons who, by virtue of their duties, must be aware of the UKUSA Agreement and its substance. In all cases, the existence of the agreement was indirectly confirmed by the nature of the answers given.

5.5. Evaluation of declassified American documents

5.5.1. Nature of documents

Under the 1966 Freedom of Information Acts (5 USC § 552) and the Department of Defense's 1997 FOIA Regulation 5400.7-R, formerly classified documents were declassified and thus made available to the public.

The documents concerning the National Security Archive, founded in 1985 at George Washington University in Washington DC, are accessible to the public. The author Jeffrey Richelson, a former member of the National Security Archive, has published 16 documents on the Internet which give an insight into the emergence, development, management and mandate of the National Security Agency (NSA).[2] In two of these documents, ECHELON is named. These documents have repeatedly been cited by various authors writing about ECHELON as evidence for the existence of the ECHELON global espionage system. The documents made available by Richelson also include some which confirm the existence of the National Reconnaissance Office and its function as a manager and operator of SIGINT satellites.[3]

[1] Andrew, Christopher 'The growth of the Australian Intelligence Community and the Anglo-American Connection', pp. 223-4.
[2] http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html
[3] http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB35/index.html

5.5.2. Content of documents

The documents contain fragmentary descriptions of or references to the following topics:

5.5.2.1. Purpose and structure of the NSA (Documents 1, 4, 10, 11 and 16)

In National Security Council Intelligence Directive 9 (NSCID 9) of 10 March 1950 the term 'foreign communications' is defined for COMINT purposes: it comprises **any government communications in the widest sense (not only military) and all other communications which might contain information of military, political, scientific or economic value.**

The Directive (NSCID 9 rev. 29.12.52) expressly states that the FBI alone is responsible for internal security.

The Department of Defense (DoD) Directive of 23 December 1991 on the NSA and the Central Security Service (CSS) outlines the concept for the NSA as follows:

- The NSA is a separately organised office within the DoD headed by the Secretary of Defense;
- The NSA's task is firstly to fulfil the USA's SIGINT mission, and secondly to provide secure communications systems for all departments and offices;
- The NSA's SIGINT activities do not cover the production and distribution of processed intelligence: this is the sphere of other departments and offices.

The 1991 DoD Directive also sketches out the structure of the NSA and CSS.

In its statement to the House Permanent Select Committee on Intelligence on 12 April 2000, Gen. Michael Hayden, the NSA Director, defined the NSA's tasks as follows:

- Collecting foreign communications for the military and for policymakers by means of electronic surveillance;
- Supplying intelligence for US Government consumers about international terrorism, drugs and arms proliferation;
- The NSA does not have the task of collecting all electronic communications.
- The NSA may only pass on information to recipients authorised by government, not direct to US firms.

In a memorandum by Vice-Admiral W.O. Studeman of the US Navy on behalf of the Government on 8 April 1992, reference was made to the increasingly global access of the NSA in addition to 'support of military operations'.

5.5.2.2. Powers of the Intelligence Agencies (Document 7)

It is clear from US Signals Intelligence Directive 18 (USSID 18) that both cable and radio signals are intercepted.

5.5.2.3. Cooperation with other services (Documents 2a and 2b)

The duties of the US Communications Intelligence Board include monitoring all 'arrangements' with foreign governments in the COMINT field. One of the tasks of the NSA Director is to arrange all contacts with foreign COMINT services.

5.5.2.4. Mention of units active in 'ECHELON sites' (Documents 9 and 12)

The NAVSECGRU Instructions C5450.48A describe the duties, function and purpose of the Naval Security Group Activity (NAVSECGRUACT), 544th Intelligence Group, in Sugar Grove, West Virginia. They state that one particular task is to 'maintain and operate an ECHELON site'; they also mention that one task is the processing of intelligence information.

In the document 'History of the Air Intelligence Agency – 1 January to 31 December 1994 (RCS:HAF-HO(A&SA)7101 Volume 1) the Air Intelligence Agency (AIA), Detachment 2 and 3, is mentioned under the heading 'Activation of ECHELON Units'.

These documents do not give any information on what an ECHELON site is, what is done at an ECHELON site, or what the code name ECHELON stands for. These documents do not reveal anything about the UKUSA Agreement.

5.5.2.5. Mention of Stations (Documents 6, 9 and 12)

- Sugar Grove, West Virginia in the NAVSECGRU Instructions C5450.48A
- Misawa Air Base, Japan, in History of the Air Intelligence Agency – 1 January to 31 December 1994 (RCS:HAF-HO(A&SA)7101 Volume 1)
- Puerto Rico (i.e. Sabana Seca), ibid.
- Guam, ibid.
- Yakima, Washington, ibid.
- Fort Meade, Maryland; a COMINT report by the NSA of 31 August 1971 from Fort George G. Meade, Maryland confirms the COMINT activities there.

5.5.2.6. Protection of the privacy of US citizens (Documents 7, 7 a to f, 11 and 16)

The NAVSECGRU Instructions C5450.48A state that the privacy of citizens must be protected.

Various documents state that the privacy of American citizens must be protected and how this is to be done (Baker, General Counsel, NSA, letter of 9 September 1992, US Signals Intelligence Directive (USSID) 18, 20 October 1980, and various supplements.[1]

[1] Dissemination of US Government Organisations and Officials, Memorandum 5 February 1993; Reporting Guidance on References to the First Lady, 9 July 1993; Reporting Guidance on Former President Carter's Involvement in the Bosnian Peace Process, 15 December 1994; Understanding USSID 18, 30 September 1997; USSID 18 Guide, 14 February 1998.

NSA/US Identities in SIGINT, March 1994: Statement for the record of NSA Director Lt Gen Michael V. Hayden, USAF, 12 April 2000.

5.5.2.7. Definitions (Documents 4, 5a and 7)

The Department of Defense Directive of 23 December 1991 provides precise definitions of SIGINT, COMINT, ELINT and TELINT, as does the National Security Council Intelligence Directive No 6 of 17 February 1972.

According to these, COMINT means the collection and processing of foreign communications (passed by electromagnetic means) up to and including the interception and processing of unencrypted written communications, press and propaganda unless encrypted.

5.5.3. Summary

1. As long as 50 years ago there was interest in information not only from the political and security spheres but also from the fields of science and economics.
2. The documents prove that the NSA works together with other services in the field of COMINT.
3. The documents which reveal information about how the NSA is organised, what tasks it has and that it is responsible to the Department of Defense, do not add any essential information beyond what can be gathered from publicly accessible sources on the NSA home page.
4. Cable communications may be intercepted.
5. The 544th Intelligence Group and Detachment 2 and 3 of the Air Intelligence Agency are involved in the collection of intelligence information.
6. The term 'ECHELON' appears in a number of contexts.
7. Sugar Grove in West Virginia, Misawa Air Base in Japan, Puerto Rica (i.e. Sabana Seca), Guam, and Yakima in Washington State are named as SIGINT stations.
8. The documents provide information on how the privacy of American citizens should be protected.

The documents do not constitute proof, but provide compelling clues which enable conclusions to be drawn when taken in conjunction with other evidence.

5.6. Information from authors and journalists specialised in this field

5.6.1. Nicky Hager's book

The ECHELON system was first described in detail in Nicky Hager's book 'Secret Powers – New Zealand's role in the international spy network', published in 1996. According to Hager, the system's origins can be traced back to 1947, when, following their cooperation in the war, the UK and USA concluded an agreement on continuing COMINT activities on a joint basis around the globe, under which the two countries were to cooperate on the creation of an interception system providing the maximum possible global coverage, share the special installations required and the associated costs and pool the fruits of their labours. Canada, Australia and New Zealand subsequently signed up to the UKUSA agreement.

Hager says that interception of satellite communications is now the system's core activity. The interception by ground stations of messages sent via Intel satellites – the first global satellite

communication system[1] - began in the 1970s. Such messages are then searched by computer for specific keywords and/or addresses in order to filter out the relevant communications. Surveillance activity was later extended to other satellites, such as those of Inmarsat[2], which concentrated on maritime communications.

In his book, Hager points out that the interception of satellite communications represents only a small, albeit important, part of the eavesdropping system, for there are also numerous facilities for monitoring microwave and cable links, although these are less well documented and their existence is more difficult to prove, since, unlike ground stations, they are rather inconspicuous. ECHELON is thus synonymous with a global eavesdropping system.

5.6.2. Duncan Campbell

In STOA Study 2/5 of 1999, which provides an in-depth analysis of the technical aspects, Duncan Campbell described in detail how any medium used for transmitting information can be intercepted. In one of his latest writings, however, he makes it clear that even ECHELON has its limits and that the initial view that total monitoring of communications was possible has turned out to be erroneous. 'Neither ECHELON nor the signals intelligence ('sigint') system of which it is part can do this. Nor is equipment available with the capacity to process and recognise the content of every speech message or telephone call.' [3]

5.6.3. Jeff Richelson

awaiting results of the discussions with him in the USA

5.6.4. James Bamford

to follow

5.6.5. Bo Elkjaer and Kenan Seeberg

These two Danish journalists told the Committee on 22 January 2001 that ECHELON was already very advanced in the 1980s and that Denmark had cooperated with the USA since 1984.

5.7. Statements by former intelligence service employees

5.7.1. Margaret Newsham (former NSA employee)

Margaret Newsham[4] was employed from 1974 to 1984 by Ford and Lockheed and says she worked for the NSA during that period. She had been trained for her work at NSA Headquarters at Fort George Meade in Maryland, USA, and had been deployed from 1977 to 1978 at Menwith Hill, the US ground station on UK territory. There she established that a conversation conducted by US Senator Strohm Thurmond was being intercepted. As early as 1978, ECHELON was

[1] See http://www.intelsat.int/index.htm
[2] See http://www.inmarsat.org/index3.html
[3] Duncan Campbell, Inside ECHELON. The history, structure and function of the global surveillance system known as ECHELON, 1
[4] See Bo Elkjaer, Kenan Seeberg, ECHELON was my baby – Interview with Margaret Newsham, Ekstra Bladet, 17.1.1999

capable of intercepting telecommunications messages to and from a particular person via satellite.

As regards her role in the NSA, she was responsible for designing systems and programs, configuring them and preparing them for operation on powerful computers. The software programs were named SILKWORTH and SIRE, whilst ECHELON was the name of the network.

5.7.2. Wayne Madsen (former NSA employee)

Wayne Madsen[1], former NSA employee, also confirms the existence of ECHELON. He is of the opinion that economic intelligence gathering has top priority and is used to the advantage of US companies. He fears in particular that ECHELON could spy on NGOs such as Amnesty International or Greenpeace. He argues that the NSA had to concede that it held more than 1000 pages of information on Princess Diana, because her conduct ran counter to US policy, owing to her campaign against land mines.

5.7.3. Mike Frost (former Canadian secret service officer)

Mike Frost worked for more than 20 years for the CSE, the Canadian secret service[2]. The listening post in Ottawa was just one part of a worldwide network of spy stations.[3] In an interview with CBS, he said that all over the world, every day, telephone conversations, e-mails and faxes are monitored by ECHELON, a secret government surveillance network.[4] This also included civilian communications. In an interview he gave for an Australian TV channel, he said by way of example that the CSE actually had entered the name and telephone number of a woman in a database of possible terrorists because she had used an ambiguous phrase in a harmless telephone conversation with a friend. When searching through intercepted communications, the computer had found the keyword and reproduced the conversation. The analyst was unsure and therefore recorded her personal details.[5]

The intelligence services of the ECHELON community also helped each other by spying on each other's behalf so that at least local intelligence services could not be accused of anything. For instance, GCHQ asked the CSE to spy on two British government ministers when Prime Minister Thatcher wanted it to tell her if they were on her side.[6]

5.7.4. Fred Stock (former Canadian secret service employee)

Fred Stock says he was expelled from CSE, the Canadian secret service, in 1993 because he had criticised the new emphasis on economic intelligence and civil targets. The communications intercepted contained information on trade with other countries, including negotiations on

[1] NBC TV interview '60 Minutes', 27.2.2000; http://cryptome.org/echelon-60min.htm
[2] Communication Security Establishment, subordinate to the Canadian Ministry of Defense, engaged in SIGINT
[3] NBC TV interview '60 Minutes', 27.2.2000; http://cryptome.org/echelon-60min.htm
[4] Rötzer, Die NSA geht wegen ECHELON an die Öffentlichkeit; http://www.heise.de/bin/tp/issue/download.cgi?artikelnr=6633&rub_ordner=special
[5] NBC TV interview '60 Minutes', 27.2.2000; http://cryptome.org/echelon-60min.htm
[6] Interview on the Australian Channel 9 on 23..3.1999; http://www.geocities.com/CapitolHill/Senate/8789/sunday1.htm

NAFTA, Chinese purchases of cereals and French arms sales. Stock says the service also routinely received communications concerning environmental protests by Greenpeace vessels on the high seas.[1]

5.8. Information from government sources

5.8.1. USA

James Woolsey, the former director of the CIA, said at a press conference[2] he gave at the request of US State Department, that the USA did conduct espionage operations in continental Europe. However, 95% of 'economic intelligence' was obtained by evaluating publicly accessible information sources, and only 5% came from stolen secrets. Espionage was used to secure economic intelligence from other countries where compliance with sanctions and dual-use goods were concerned, and in order to combat bribery in connection with the award of contracts. Such information is not, however, passed to US companies. Woolsey stressed that, even if espionage yielded economically usable intelligence, it would take an analyst a very long time to analyse the large volume of available information, and that it would be wrong to use their time on spying on friendly trading partners. He also pointed out that, even if they did so, complex international interlinkages would make it difficult to decide which companies were US companies and thus should be allowed to have the information.

In a later article for the Wall Street Journal Europe[3], Woolsey again said that the USA was spying on Europe, but only in order to expose cases of bribery. He stated quite clearly that the USA used computers to perform keyword searches of data.

5.8.2. UK

Answers to various questions in the House of Commons[4] reveal that the station at RAF Menwith Hill is owned by the UK Ministry of Defence, but is made available to the US Department of Defense, specifically the NSA[5], which provides the chief of station,[6] as a communications facility.[7] In mid-2000, there were 415 US military, 5 UK military, 989 US civilian and 392 UK civilian personnel working at RAF Menwith Hill, excluding GCHQ staff present on the site.[8] The presence of US military personnel is governed by the North Atlantic Treaty and special confidential[9] administrative arrangements appropriate to the relationship which exists between the governments of the UK and the USA for the purposes of common defence.[10] The station is an integral part of the US Department of Defense's worldwide network which supports the interests of the UK, the USA and NATO.[11]

---

[1] Bronskill, Canada a key snooper in huge spy network, Ottawa Citizen, 24.10.2000, http://www.ottawacitizen.com/national/990522/2630510.html
[2] Transcript, 7.3.2000, http://cryptome.org/echelon-cia.htm
[3] James Woolsey, Why America Spies on its Allies, The Wall Street Journal, 22.3.2000, 31
[4] Commons Written Answers, House of Commons Hansard Debates
[5] 12.7.1995.
[6] 25.10.1994
[7] 3.12.1997
[8] 12.5.2000
[9] 12.7.1995
[10] 8.3.1999, 6.7.1999
[11] 3.12.1997

In the Intelligence and Security Committee's 1999/2000 annual report, emphasis is specifically placed on the value of the close cooperation under the UKUSA agreement, as reflected in the quality of the intelligence gathered. It is pointed out in particular that when the NSA's equipment was out of action for some three days, US customers as well as UK customers were served direct from GCHQ.[1]

5.8.3. Australia[2]

Martin Brady, Director of the Australian intelligence service DSD[3], confirmed in a letter to the 'Sunday' programme on Australia's Channel 9 that DSD cooperated with other intelligence services as part of the UKUSA agreement. In the same letter, he stressed that all Australia's intelligence facilities were operated by Australian services alone or jointly with US services. Where use of such facilities is shared, the Australian Government has full knowledge of all activities and Australian personnel is involved at all levels.[4]

5.8.4. Netherlands

On 19 January 2001, the Netherlands Minister for Defence presented a report to the Netherlands Parliament on technical and legal aspects of the global surveillance of modern telecommunications systems.[5] In it, the Netherlands Government takes the view that, although it had no information of its own on this matter, it was highly likely, on the basis of available third-party information, that the ECHELON network did exist, but that there were also other systems with the same capabilities. The Netherlands Government came to the conclusion that global interception of communications systems was not confined to countries involved in the ECHELON system, but was also carried on by government authorities of other countries.

5.8.5. Italy

Luigi Ramponi, former director of SISMI, the Italian intelligence service, leaves no room for doubt in the interview he gave for 'Il Mondo' that ECHELON does exist.[6] Ramponi says explicitly that, as Head of SISMI, he knew of ECHELON's existence. Since 1992, he had been kept in the picture about intensive interception of low-, medium- and high frequencies. When he joined SISMI in 1991, most dealings were with the UK and the USA.

---

[1] Intelligence and Security Committee, Annual Report 1999-2000, para. 14, presented to parliament by the Prime Minister in November 2000.

[2] http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp;
http://sunday.ninemsn.com/01_cover_stories/article_335.asp

[3] Defence Signals Directorate, Australian intelligence service engaged in SIGINT

[4] Letter of 16.3.1999 from Martin Brady, Director of the DSD, to Ross Coulthart, 'Sunday' programme; see also:
http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp;
http://sunday.ninemsn.com/01_cover_stories/article_335.asp

[5] Brief aan de Tweede Kamer betreffende 'Het grootschalige afluisteren van moderne telecommunicatiesystemen', 19.1.2001

[6] Francesco Sorti, Dossier. exclusivo. caso ECHELON. parla Luigi Ramponi. Anche I politici sapevano, il mondo, 17.4.1998

5.9. Parliamentary reports

5.9.1. Reports by the Comité Permanent R, Belgium's monitoring committee

The Belgian monitoring committee, the Comité Permanent R, has already discussed ECHELON in two reports.

The third chapter of its 1999 activity report was devoted to how the Belgian intelligence services are reacting to the possible existence of an ECHELON system of communications surveillance. The 15-page report concludes that both the Belgian intelligence services, the Sûreté de l'Etat and the Service General du Renseignement (SGR), only found out about ECHELON through documents in the public domain.

The second report (rapport complémentaire d'activités 1999) deals with the ECHELON system in much greater detail. It gives a view on the STOA study and devotes one section to explaining the technical and legal background to telecommunications monitoring. It concludes that ECHELON does in fact exist and is also in a position to listen in to all information carried by satellite (approximately 1% of total international telephone communications), in that it searches for keywords, and that its decoding capacity is much greater than the Americans claim. Doubt remains about the accuracy of statements that no industrial espionage is carried out at Menwith Hill. The report makes it clear that it is impossible to ascertain with any certainty what ECHELON does or does not do.

5.9.2. Report by the French National Assembly's Committee on National Defence

The French National Assembly's Committee on National Defence has drawn up a report on surveillance systems[1].

Following a detailed discussion of a wide variety of aspects, the rapporteur, Arthur Paecht, comes to the conclusion that ECHELON exists and is, in his view, the only known multinational surveillance system. The system's capacities are real but have reached their limits not only because the expenditure can no longer keep pace with the explosion in communications but also because certain targets now know how to protect themselves.

The ECHELON system has moved away from its original goals, which were linked to the Cold War, and this means that it is not impossible that the intelligence gathered may be used for political and industrial purposes against other Nato states.

ECHELON might indeed present a danger to fundamental freedoms and in this context it raises numerous problems that demand appropriate answers. It would be wrong to imagine that the ECHELON member states will give up their activities. On the contrary, there are several indications of a new system being created with new partners as a way of acquiring additional resources to overcome ECHELON's limits.

[1] Rapport d'information déposé en application de l'article 145 du règlement par la commission de la défense nationale et des forces armées, sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale, No 2623 Assemblée nationale, enregistré à la Présidence de l'Assemblée nationale le 11 octobre 2000.

6. Might there be other global interception systems?

6.1. Requirements of such a system

6.1.1. Technical and geographical requirements

Listening in to international communications transmitted by first-generation satellites requires receiving stations in the Atlantic, the Indian Ocean and the Pacific area. In the case of the newer generation of satellites, which can transmit to sub-regions, further requirements with regard to the geographical position of listening stations would have to be met if all communications via satellite were to be intercepted.

Any other interception system operating on a global scale would be forced to establish its stations outside the territory of the ECHELON states.

6.1.2. Political and economic requirements

The establishment of an interception system of this kind operating on a global scale would, however, also have to make economic and political sense for the operator or operators. The beneficiary or beneficiaries of such a system would have to have global economic, military or other security interests, or at least believe that they were among the world's superpowers. Consequently, we are essentially talking only about China and the G-8 States, excluding the United States and the UK.

6.2. France

France has its own territories, departments and regional authorities in all three areas listed above.

In the Atlantic, there is St Pierre and Miquelon east of Canada (65º W/47º N), Guadeloupe, north-east of South America (61º W/16º N), and Martinique (60º W/14º N) and French Guyana on the north-east coast of South America (52º W/5º N).

In the Indian Ocean there is Mayotte to the east of southern Africa (45º E/12º S) and Réunion (55º E/20º S) and to the very south the French Southern and Antarctic Territories. In the Pacific there is New Caledonia (165º E/20º S), the Wallis and Futuna Islands (176º W/12º S) and French Polynesia (150º W/16º S).

Very little information is available about possible stations operated by the French intelligence service (DGSE) in these overseas areas. According to reports by French journalists[1], there are stations in Kourou in French Guyana and in Mayotte. No details are available as to the size of the stations, the number of satellite antennae or their size. There are apparently other stations in France at Domme near Bordeaux and at Alluetts-le-Roi near Paris. Vincent Jauvert estimates that there is a total of 30 satellite dishes. The author Schmidt-Enboom[2] claims that a station is also operating in New Caledonia.

Theoretically, France could also operate a global interception system. However, there is insufficient information available in the public domain for your rapporteur to seriously assume that this is the case.

6.3. Russia

The Russian intelligence service FAPSI, which is responsible for communications security and SIGINT, apparently operates ground stations in Latvia, Vietnam and Cuba in cooperation with the Russian military intelligence service GRU.

In the Atlantic area, the Federation of American Scientists claims that there is a facility at Lourdes in Cuba (82º W/23º N), which is operated jointly with the Cuban intelligence service. In the Indian Ocean there are stations in Russia, about which no further information is available, and a station in Skundra in Latvia. In the Pacific there is apparently a station at Cam Rank Bay in North Vietnam. No detailed information is available about the stations as far as the number and size of the antennae are concerned.

Together with the stations available in Russia itself, global coverage is theoretically possible. However, here too, the information available is insufficient to draw any firm conclusions.

6.4. The other G-8 States and China

Neither the other G-8 States or China have territories or close allies in the parts of the world that would enable them to operate a global interception system.

[1] Jean Guisnel, Léspionage nést plus un secret, The Tocqueville Connection, 10.7.1998.
Vincent Jauvert, Espionnage comment la France, Le Nouvel Observateur, 5.4.2001, No 1900, p. 14 et seq.
[2] E.Schmidt-Eenboom, in: Streng Geheim, Museumsstiftung Post und Telekommunikation, Heidelberg 1999, p.180.

7. Compatibility of an 'ECHELON' type communications interception system with Union law

7.1. Preliminary considerations

The committee's remit includes the specific task of examining the compatibility of an 'ECHELON' type communications interception system with Community law[1]. In particular, it is to examine whether such a system complies with the two data protection directives 95/46/EC and 97/66/EC, with Article 286 TEC, and Article 8(2) TEU.

This matter has to be considered from two different angles. The first arises from the circumstantial evidence set out in Chapter 5, which indicates that the system known as 'ECHELON' was designed as a communications interception system to provide the US, Canadian, Australian, New Zealand and British secret services with information about events abroad by collecting and evaluating communications data. As such, it is a conventional espionage tool used by foreign intelligence services[2]. Initially, therefore, we will examine the compatibility of such an intelligence system with Union law.

In addition, the STOA report by Duncan Campbell alleges that the system has been misused for purposes of obtaining competitive intelligence, causing serious losses to the industries of European countries. Furthermore, there are statements by the former CIA Director R. James Woolsey, that although the USA was spying on European firms, this was only to restore a level playing field since contracts had only been secured as a result of bribery[3]. If it is true that the system is used to obtain competitive intelligence, the further issue arises of whether this is compatible with Community law. This second aspect will therefore be discussed separately.

7.2. Compatibility of an intelligence system with Union law

7.2.1. Compatibility with EC law

In principle, activities and measures undertaken for the purposes of state security or law enforcement do not fall within the scope of the EC Treaty. As, on the basis of the principle of limited authority, the European Community can only take action where a corresponding competence has been conferred on it, the Community rightly excluded these areas from the scope of application of the data protection directives, which are based on the EC Treaty, and in particular Article 95 (ex-Article 100a) thereof. Directive 59/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data[4] and Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector[5] do not apply to 'the processing of data[1]/activities[2]

[1] See Chapter 1, 1.3 above.

[2] See Chapter 2.

[3] *See Chapters 5, 5.6. and 5.8.*

[4] OJ L 281 1995 p. 31.

[5] OJ L 24 1998 p.1.

concerning public security, defence, state security (including the economic well-being of the state when the activities relate to state security matters) and the activities of the state in areas of criminal law'. Exactly the same wording has been used in the proposal for a directive concerning the processing of personal data and the protection of privacy in the electronic communications sector[3] which is currently before Parliament. The involvement of a Member State in an interception system for the purposes of State security cannot therefore be in breach of the data protection directives.

Similarly, there can be no breach of Article 286 TEC, which extends the scope of the data protection directives to data processing by Community institutions and bodies. The same applies to Regulation 45/2001on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[4]. This regulation is also applicable only in so far as the bodies are acting within the framework of the EC Treaty[5]. To avoid misunderstandings, it should be clearly emphasised at this point that no sources whatsoever contend that there is any involvement of Community bodies and institutions in a surveillance system and the rapporteur has absolutely no grounds for assuming this to be the case.

7.2.2. Compatibility with other EU law

As far as the areas covered by Title V (common foreign and security policy) and Title VI (police and judicial cooperation in criminal matters) are concerned, there are no data protection provisions comparable to those of the EC directives. The European Parliament has already pointed out on numerous occasions that action is much needed in this area[6].

The protection of the fundamental rights and freedoms of the individual in these spheres is ensured only by Articles 6 and 7, in particular by Article 6(2) TEU, in which the Union undertakes to respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and as they derive from the constitutional traditions common to the Member States. Not only are fundamental rights, and in particular the ECHR, binding on the Member States (see Chapter 8), but the Union is also required to comply with fundamental rights in its legislation and administration. However, since at EU level there are still no regulations concerning the admissibility of the interception of

---

[1] Art 3(2) Regulation 95/46.
[2] Art 1(1) Regulation 97/66.
[3] COM (2000) 385 final, OJ C 365 E/223.
[4] Regulation (EC) No 45/2001, OJ L 8, p.1.
[5] Art 3(1) and Recital 15 "Where such processing is carried out by Community institutions or bodies in the exercise of activities falling outside the scope of this Regulation, in particular those laid down in Titles V and VI of the Treaty on European Union, the protection of individuals' fundamental rights and freedoms shall be ensured with due regard to Article 6 of the Treaty on European Union."
[6] See, for example, para 25 of the resolution on the draft action plan of the Council and Commission on how best to implement the provisions of the Treaty of Amsterdam on an area of freedom, security and justice (13844/98 - C4-0692/98 - 98/0923(CNS)), OJ C 219, 30.7.1999, p. 61 et seq.

telecommunications for security or intelligence purposes[1], the issue of infringement of Article 6(2) TEU does not yet arise.

7.3. The question of compatibility in the event of misuse of the system for industrial espionage

If a Member State were to promote the use of an interception system, which was also used for industrial espionage, by allowing its own intelligence service to operate such a system or by giving foreign intelligence services access to its territory for this purpose, it would undoubtedly constitute a breach of EC law. Under Article 10 TEC, the Member States are committed to acting in good faith and, in particular, from abstaining from any measure which could jeopardise the attainment of the objectives of the Treaty. Even if the interception of telecommunications is not carried out for the benefit of the domestic industry (which would, in fact, be equivalent in effect to State aid, and thus in breach of Article 87 TEC), but for the benefit of a non-member state, activities of this kind would be fundamentally at odds with the concept of a common market underpinning the EC Treaty, as it would amount to a distortion of competition.

In the opinion of the rapporteur, action of this kind would also be an infringement of the data protection directives for the telecommunications sphere[2], since the question of the applicability of the directive has to be resolved from a functional rather than an organisational point of view. This follows not only from the wording of the regulation as regards its scope, but also from the sense of the law. If intelligence services use their capability for industrial espionage, these activities are not being carried out for the purposes of security or law enforcement but for other purposes and would consequently fall fully within the scope of the directive. Article 5 of the directive requires the Member States to ensure the confidentiality of communications. 'In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users'. Pursuant to Article 14, exceptions may be made only where they are necessary to safeguard national security, defence and law enforcement. As industrial espionage is no justification for an exception, it would, in this case, constitute an infringement of Community law.

7.4. Conclusion

To sum up, it can therefore be said that the current legal position is that an ECHELON type intelligence system is not in breach of Union law because it does not concern the aspects of Union law that would be required for there to be incompatibility. However, this applies only where the system is actually used exclusively for the purposes of state security. On the other

[1] In the area of telecommunications surveillance there are currently only two EU legislative acts, neither of which covers the question of admissibility:
- Council resolution of 17 January 1995 on the lawful interception of telecommunications (OJ C 329, 4.11.1996), the annex to which sets out the technical requirements relating to the lawful interception of modern telecommunications systems, and
- Council Act of 29 May 2000 establishing, in accordance with Article 34 of the Treaty on European Union, the Convention on mutual assistance in criminal matters between the Member States of the European Union (OJ 2000 C 197/1, Art 17), which regulates the conditions under which mutual assistance in criminal matters with regard to telecommunications interception is possible. These provisions in no way curtail the rights of the subjects of tapping as the Member State in which the subject is to be found has the right to refuse mutual assistance if it is not authorised under national law.

[2] Regulation 97/66 EC, OJ L 24 1998, p.1.

hand, were it to be used for other purposes and for industrial espionage directed against foreign firms, this would constitute an infringement of EC law. Were a Member State to be involved in such action, it would be in breach of Community law.

8. The compatibility of communications surveillance by intelligence services with the fundamental right to privacy

8.1. Communications surveillance as a violation of the fundamental right to privacy

Any act involving the interception of communications, and even the recording of data by intelligence services for that purpose[1], represents a serious violation of an individual's privacy. Only in a 'police state' is the unrestricted interception of communications permitted by government authorities. In contrast, in the EU Member States, which are mature democracies, the need for state bodies, and thus also intelligence services, to respect individuals' privacy is unchallenged and is generally enshrined in national constitutions. Privacy thus enjoys special protection: potential violations are authorised only following analysis of the legal considerations and in accordance with the principle of proportionality.

The ECHELON states are also well aware of the problem. However, these states' protection provisions are geared to respect for the privacy of their own inhabitants, so that as a rule European citizens do not benefit from them in any way. For example, the US provisions which lay down the conditions governing electronic surveillance do not set the state's interest in operating a properly functioning intelligence service against the interests of effective, general protection fundamental rights, but rather against the need to protect the privacy of 'US persons'[2].

8.2. The protection of privacy under international agreements

Many agreements under international law specify respect for privacy as a fundamental right[3]. At world level, particular mention should be made of the International Covenant on Civil and Political Rights[4], which was adopted by the UN in 1966. Article 17 of the Covenant guarantees the protection of privacy. In connection with complaints submitted by other states, all the ECHELON states have complied with the decisions taken by the Human Rights Committee set up pursuant to Article 41 of the Covenant to rule on breaches of the Covenant under international

[1] German Federal Constitutional Court (FCC), 1 BVR 226/94 of 14 July 1999, Rz 187: 'The recording of data already represents a violation of that right in so far as it makes the content of the communications available to the Federal Intelligence Service and forms the basis of the ensuing analysis using search terms'.

[2] Compare the report submitted to the US Congress in late February 2000, 'Legal Standards for the Intelligence Community in Conducting Electronic Surveillance', http://www.fas.org/irp/nsa/standards.html, which refers to the Foreign Intelligence Surveillance Act (FISA), printed in Title 50, Chapter 36, USC, § 1801 et seq, and Executive Order No 12333, 3 CFR 200 (1982), printed in Title 50, Chapter 15, USC, § 401 et seq, http://www4.law.cornell.edu/uscode750/index.html.

[3] Article 12 of the Universal Declaration of Human Rights; Article 17 of the UN Covenant on Civil and Political Rights; Article 7 of the EU Charter of Fundamental Rights; Article 8 of the ECHR; Recommendation of the OECD Council on guidelines for the security of information systems, adopted on 26/27 November 1993, C(1992) 188/final; Article 7 of the Council of Europe Convention on the Protection of Persons with regard to the automatic processing of personal data; compare the study commissioned by STOA entitled 'Development of Surveillance Technology and Risk of Abuse of Economic Information; Vol. 4/5: the legality of the interception of electronic communications: a concise survey of the principal legal issues and instruments under international, European and national law (Chris Elliot), October 1999, 2.

[4] Adopted by the UN General Assembly on 16 December 1966.

law. The Optional Protocol[1], which extends the powers of the Human Rights Committee to cover complaints submitted by private individuals, has not been signed by the USA, however, so that such individuals cannot appeal to the Human Rights Committee in the event of the violation of the Covenant by the USA.

At EU level, efforts have been made to establish specifically European arrangements for the protection of fundamental rights through the drafting of a Charter of Fundamental Rights of the EU. Article 7 of the Charter, entitled 'Respect for private and family life', even lays down explicitly in law the right to respect for communications[2]. In addition, Article 8 lays down in law the fundamental right to the 'protection of personal data'. This would have protected individuals in those cases involving the (computerised or non-computerised) processing of their data, something which generally occurs when voice communications are intercepted and invariably does when other forms of communication are intercepted.

However, since no provision has been made for the incorporation of the Charter into the Treaty, at least as part of the forthcoming reform, the Charter offers European citizens no additional protection. The signing of the Charter by the Presidents of Parliament, the Commission and the Council on 7 December 2000 may well have been politically significant; in legal terms, however, it amounts to nothing more than a statement by the institutions that they feel bound to respect the fundamental rights enshrined in the Charter.

The only effective international instrument for the comprehensive protection of privacy is the ECHR.

8.3. The rules laid down in the (ECHR)

8.3.1. The importance of the ECHR in the EU

The protection of fundamental rights provided by the ECHR is particularly important in that the Convention has been ratified by all the EU Member States, thereby creating a uniform level of protection in Europe. The contracting parties have given an undertaking under international law to guarantee the rights enshrined in the ECHR and have declared that they will comply with the judgments of the European Court of Human Rights in Strasbourg. The relevant national legal provisions can thus be reviewed by the European Court of Human Rights as to their conformity with the ECHR and, in the event of a breach of human rights, a judgment may be handed down against the contracting party concerned and it may be required to pay compensation. The ECHR has gained further in importance by being repeatedly invoked by the CJEC, alongside the general legal principles adhered to by the Member States, when that body takes decisions in cases involving legal reviews. Moreover, following the adoption of the Treaty of Amsterdam Article 6(2) of the Treaty on European Union commits the EU to respecting fundamental rights as enshrined in the ECHR.

[1] Optional Protocol to the International Covenant on Civil and Political Rights, adopted by the UN General Assembly on 16 December 1966.
[2] 'Everyone has the right to respect for his or her private family life, home and communications.'

8.3.2. The geographical and personal scope of the protection provided under the ECHR

The rights enshrined in the ECHR represent generally recognised human rights and are thus not linked to nationality. They must be granted to all persons covered by the jurisdiction of the contracting parties. In other words, the human rights in question must at all events be guaranteed throughout the territory of the contracting parties, so that local exceptions would represent a breach of the Convention. In addition, however, they are also valid outside the territory of the contracting parties, provided that state authority is exercised in such places. The rights guaranteed by the ECHR vis-à-vis a contracting state are thus also enjoyed by persons outside the territory of that state if those persons suffer interference in the exercise of their right to privacy[1].

The latter point is particularly important here, since a specific characteristic of the issue of fundamental rights in the area of telecommunications surveillance is the fact that there may be a substantial geographical distance between the state responsible for the surveillance, the person under surveillance and the location in which interception is actually carried out. This applies in particular to international communications, but may also apply to national communications if information is transmitted via connections situated abroad. Indeed, this is typical of interceptions carried out by foreign intelligence services. It is also possible that information obtained by an intelligence service by means of surveillance will be passed on to other states.

8.3.3. The admissibility of telecommunications surveillance pursuant to Article 8 of the ECHR

Pursuant to Article 8(1) of the ECHR, 'everyone has the right to respect for his private and family life, his home and his correspondence'. No explicit reference is made to the protection of telephony or telecommunications, but, under the terms of the case law of the European Court of Human Rights, they are protected by the provisions of Article 8, since they are covered by the concepts of 'private life' and 'correspondence'[2]. The scope of the protection of this fundamental right covers not only the substance of the communication, but also the act of recording external data. In other words, even if the intelligence service merely records data such as the time and duration of calls and the numbers dialled, this represents a violation of privacy[3].

Pursuant to Article 8(2) of the ECHR, exercise of this fundamental right is not unrestricted. Interference in the exercise of the fundamental right to privacy may be admissible if there is a

[1] See the judgment of the European Court of Human Rights, Loizidou/Turkey, 23.3.1995, line 62, with further references: '… the concept of "jurisdiction" under this provision is not restricted to the national territory of the High Contracting Parties […] responsibility can be involved because of acts of their authorities, whether performed within or outside national boundaries, which produce effects outside their own territory', with reference to the European Court of Human Rights, Drozd and Janousek, 26.6.1992, line 91. See also the comprehensive details in Jacobs, the European Convention on Human Rights (1996), pp. 21 et seq.

[2] See European Court of Human Rights, Klass et al, 6.1978, line 41.

[3] See European Court of Human Rights, Malone, 2.8.1984, line 83 et seq; also B. Davy/U.Davy, Aspects of state information collection and Article 8 of the ECHR, JBl 1985, 656.

legal basis under national law[1]. The law must be generally accessible and its consequences must be foreseeable[2].

In that connection, the Member States are not free to interfere in the exercise of this fundamental right as they see fit. They may do so only for the purposes listed in the second paragraph of Article 8 of the ECHR, in particular in the interests of national security, public safety or the economic well-being of the country[3]. However, this does not justify industrial espionage, since it only covers forms of interference 'necessary in a democratic society'. In connection with any instance of interference, the least invasive means appropriate must be employed to achieve the objective; in addition, adequate guarantees must be laid down to prevent misuse of this power.

8.3.4. The significance of Article 8 of the ECHR for the activities of intelligence services

These general principles have the following implications for the organisation of the work of intelligence services in a manner consistent with this basic right: if, for the purpose of safeguarding national security, there seems to be a need to authorise intelligence services to record the substance of telecommunications, or at least external data relating to the connections in question, this power must be established in national law and the relevant provisions must be generally accessible. The consequences for individuals must be foreseeable, but due account must be taken of the particular requirements in the sphere of national security. Accordingly, in a ruling on the conformity with Article 8 of secret checks on employees in areas relating to national security, the European Court of Human Rights noted that in this special case the arrangements governing the foreseeability requirement must differ from those in other areas[4]. In this context as well, however, it stipulated that the law must at all events state under what circumstances and subject to what conditions the state may carry out secret, and thus potentially dangerous, interference in the exercise of the right to privacy[5].

In connection with the organisation of the activities of intelligence services in a manner consistent with human rights, due account must be taken of the fact that, although national security can be invoked to justify an invasion of privacy, the principle of proportionality, as defined in Article 8(2) of the ECHR, also applies: national security represents valid grounds only in cases where action to protect it is necessary in a democratic society. In that connection, the European Court of Human Rights has clearly stated that the interest of the state in protecting its national security must be weighed up against the seriousness of the invasion of an individual's privacy[6]. Invasions of privacy may not be restricted to the absolute minimum, but mere

[1] Under the case law of the European Court of Human Rights (in particular Sunday Times, 26.4.1979, line 47 et seq, Silver et al, 25.3.1983, line 85 et seq, the term 'the law' in Article 8(2) embraces not only laws in the formal sense, but also legal provisions below the level of a law and, in certain circumstances, even unwritten law. It is essential, however, that it is clear to the legal subject under what circumstances interference is possible. See Wessley, Telecommunications Privacy – an unknown basic right?, ÖJZ 1999, pp. 491 et seq, 495.

[2] Silver et al, 25.3.1983, line 87 et seq.

[3] The justification of 'economic well-being' was accepted by the European Court of Human Rights in a case involving the transmission of medical data relevant to the award of public compensation, M.S./Sweden, 27.8.1997, line 38; and in a case involving the expulsion from the Netherlands of a person who had been living on welfare payments after the grounds for the award of a residence permit had ceased to apply, Ciliz/Netherlands, 11.7.2000, line 65.

[4] European Court of Human Rights, Leander, 26.3.1987, line 51.

[5] European Court of Human Rights, Malone, 2.8.1984, line 67.

[6] European Court of Human Rights, Leander, 26.3.1987, line 59, Sunday Times, 26.4.1979, line 46 et seq.

usefulness or desirability is not sufficient justification[1]. The view that the interception of all telecommunications, even if permissible under national law, represents the best form of protection against organised crime would amount to a breach of Article 8 of the ECHR.

In addition, given the specific nature of the activities conducted by intelligence services, activities which demand secrecy and, therefore, a particularly careful weighing-up of interests, provision must be made for more stringent monitoring arrangements. The European Court of Human Rights has explicitly drawn attention to the fact that a secret surveillance system operated for the purpose of protecting national security carries with it the risk that, under the pretext of defending democracy, it may undermine or even destroy the democratic system, so that more appropriate and more effective guarantees are needed to prevent such misuse of powers[2]. Accordingly, the legally authorised activities of intelligence services are only consistent with fundamental rights if the ECHR contracting party has established adequate systems of checks and other guarantees to prevent the misuse of powers.

In connection with the activities of Sweden's intelligence services, the European Court of Human Rights emphasised the fact that it attaches particular importance to the presence of MPs in police supervisory bodies and to supervision by the Minister of Justice, the parliamentary Ombudsman and the parliamentary Committee on Legal Affairs. Against this background, it must be regarded as unsatisfactory that France, Greece, Ireland, Luxembourg and Spain have no parliamentary committee with responsibility for monitoring the secret services[3] and have made no move to set up a supervisory system similar to the office of parliamentary Ombudsman pioneered by the Nordic states[4]. Your rapporteur therefore welcomes the efforts made by the French National Assembly Committee on National Defence to set up a monitoring committee[5], particularly as France has exceptional intelligence capabilities, in both technical and geographical terms.

8.4. The requirement to monitor closely the activities of other countries' intelligence services

8.4.1. Inadmissibility of moves to circumvent Article 8 of the ECHR through the use of other countries' intelligence services

As outlined in detail above, the contracting parties must comply with a set of conditions in order to demonstrate that the activities of their intelligence services are compatible with Article 8 of the ECHR. It is quite obvious that intelligence services cannot be allowed to circumvent these requirements by employing assistance from other intelligence services subject to less stringent rules. Otherwise, the principle of legality, with its twin components of accessibility and foreseeability, would become a dead letter and the case law of the European Court of Human Rights would be deprived of its substance.

[1] European Court of Human Rights, Silver et al, 24.10.1983, line 97.
[2] European Court of Human Rights, Leander, 26.3.1987, line 60.
[3] Your rapporteur is aware that neither Luxembourg nor Ireland has a foreign intelligence service and does not carry out SIGINT operations. The need for a specific supervisory body relates here only to domestic intelligence activities.
[4] For details of the situation regarding the supervision of intelligence services in the Member States, see Chapter 9.
[5] See the bill entitled 'Proposition de loi tendant à la création de délégations parlementaires pour le renseignement', and the related report by Mr Arthur Paecht, No 1951, National Assembly, 11th parliamentary term, registered on 23 November 1999.

The first implication of this is that exchanges of data between intelligence services are permissible only on a restricted basis. An intelligence service may seek from one of its counterparts only data obtained in a manner consistent with the conditions laid down in its own national law. The geographical scope for action laid down by law in respect of the intelligence service concerned may not be extended by means of agreements with other services. By the same token, it may carry out operations on behalf of another country's intelligence service, in accordance with the latter's instructions, only if it is satisfied that the operations are consistent with the national law of its own country. Even if the information is intended for another country, this in no way alters the fact that an invasion of privacy which could not be foreseen by the legal subject concerned constitutes a violation of fundamental rights.

The second implication is that states which are ECHR contracting parties may not allow other countries' intelligence services to carry out operations on their territory if they have reason to believe that those operations are not consistent with the conditions laid down by the ECHR[1].

8.4.2. Implications of allowing non-European intelligence services to carry out operations on the territory of Member States which are ECHR contracting parties

8.4.2.1. The relevant case law of the European Court of Human Rights

By ratifying the ECHR the contracting parties undertook to subject the exercise of their sovereignty to a review of its consistency with fundamental rights. They cannot seek to circumvent this requirement by foregoing the exercise of that sovereignty. These states remain responsible for their territory and thus have an obligation to European legal subjects if the exercise of sovereignty is usurped by the activities of the intelligence services of another state. The established case law of the European Court of Human Rights now emphasises that the contracting parties have a duty to take positive measures to protect privacy, in order to ensure that private individuals (!) do not violate Article 8 of the ECHR. In other words, they must take action even at a horizontal level, where private individuals are not confronted with the actions of the state, but rather of other private individuals[2]. If a state allows another country's intelligence service to work on its territory, the protection requirement is much greater, because in that case another authority is exercising its sovereignty. The only logical conclusion is that states must carry out checks to ensure that the activities of intelligence services on their territory do not represent a violation of human rights.

8.4.2.2. Implications for stations

In Bad Aibling in Germany an area of land has been declared US territory for the sole purpose of housing a satellite receiving facility. In Menwith Hill in the United Kingdom authorisation has been given for the shared use of land for the same purpose. If, in these stations, an American intelligence service were to engage in the interception of non-military communications conducted by private individuals or firms from an ECHR contracting party, supervisory requirements would come into play under the ECHR. In practical terms, as ECHR contracting

[1] See also Yernault 'ECHELON and Europe. The protection of privacy against communications espionage', Journal of the Courts, European Law, 2000, 187 et seq.

[2] European Court of Human Rights, Abdulaziz, Cabales and Balkandali, 28.5.1985, line 67; X and Y/Netherlands, 26.3.1985, line 23; Gaskin v United Kingdom, 7.7.1989, line 38; Powell and Rayner, 21.2.1990, line 41.

parties Germany and the United Kingdom are required to establish that the activities of the American intelligence services do not represent a violation of fundamental rights. This is all the more relevant because representatives of NGOs and the press have repeatedly expressed concerns regarding the activities of the US National Security Agency (NSA).

8.4.2.3. Implications for interception carried out on behalf of third parties

According to information available to the committee, in Morwenstow in the United Kingdom GCHQ, working in cooperation with the NSA and in strict accordance with the latter's instructions, intercepts civilian communications and passes on the recordings to the USA as raw intelligence material. The requirement to check that interception operations are consistent with fundamental rights also applies to work carried out on behalf of third parties.

8.4.2.4. Particular duty of care in connection with third states

In the case of operations involving two ECHR contracting parties, both can assume, up to a certain point, that the other is complying with the ECHR. At all events, this applies until evidence emerges that an ECHR contracting party is violating the Convention on a systematic, long-term basis. Things are very different, however, in the case of the USA: it is not an ECHR contracting party and it has not made its intelligence operations subject to a similar supervisory system. There are very precise rules governing the activities of its intelligence services, in so far as those activities concern US citizens or persons legally present on US territory. However, other rules apply to the activities of the NSA abroad, and many of the relevant rules are classified and thus inaccessible to the public. A further fact gives greater cause for concern, namely that although the US intelligence service is subject to monitoring by the relevant House of Representatives and Senate committees, these committees show little interest in the activities of the NSA abroad.

There would seem to be good reason, therefore, to call on Germany and the United Kingdom to take their obligations under the ECHR seriously and to make the authorisation of further intelligence activities by the NSA on their territory contingent on compliance with the ECHR. In this connection, three main factors must be considered.

1. Under the terms of the ECHR, interference in the exercise of the right to privacy may only be carried out on the basis of legal rules which are generally accessible and whose implications for individuals are foreseeable. This requirement can be met only if the USA discloses to the public in Europe how and under what circumstances intelligence-gathering is carried out. If incompatibilities with the ECHR emerge, US rules must be brought into line with the level of protection provided in Europe.

2. Under the terms of the ECHR, interference in the exercise of the right to privacy must be proportional and, in addition, the least invasive methods must be chosen. As far as European citizens are concerned, an operation constituting interference carried out by a European intelligence service must be regarded as less serious than one conducted by an American intelligence service, since only in the first instance is legal redress available in the national

courts[1]. Operations constituting interference must therefore be carried out, as far as possible, by the German or UK authorities, particularly when investigations are being conducted for law enforcement purposes . The American authorities have repeatedly tried to justify the interception of telecommunications by accusing the European authorities of corruption and taking bribes[2]. It should be pointed out to the Americans that all EU Member States have properly functioning criminal justice systems. If there is evidence that crimes have been committed, the USA must leave the task of law enforcement to the host countries. If there is no such evidence, surveillance must be regarded as unproportional, a violation of human rights and thus inadmissible. In other words, compliance with the ECHR can be guaranteed only if the USA restricts itself to surveillance measures conducted for the purpose of safeguarding its national security, but not for law enforcement purposes.

3. As already outlined above, in its case law the European Court of Human Rights has stipulated that compliance with fundamental rights is contingent on the existence of adequate monitoring systems and guarantees against abuse. This implies that US telecommunications surveillance operations carried out on European territory are consistent with human rights only if the USA introduces appropriate, effective checks on such operations carried out for the purpose of safeguarding its national security or if the NSA makes its operations on European territory subject to the authority of the control bodies set up by the host state, i.e. Germany or the United Kingdom.

The conformity of US telecommunications interception operations with the ECHR can only be guaranteed and the uniform level of protection provided in Europe by the ECHR can only be maintained if the requirements set out in the three points above are met.

[1] This is also necessary for compliance with Article 13 of the ECHR, which grants the person whose privacy has been invaded the right to submit a complaint to national courts.
[2] Woolsey (former CIA Director), Why America Spies on its Allies, The Wall Street Journal Europe, 22 March 2000, 31.

9. Are EU citizens adequately protected against the activities of intelligence services?

9.1. Protection against the activities of intelligence services: a task for the national parliaments

Although the activities of intelligence services may be covered by the CFSP in future, as yet no relevant rules have been drawn up at EU level[1], so that any arrangements to protect citizens against the activities of intelligence services can only be made under national legal systems.

In this connection, the national parliaments have a dual role to play: as legislators, they take decisions on the nature and powers of the intelligence services and the arrangements for monitoring their activities. As outlined in detail in the previous chapter, when dealing with the issue of the admissibility of telecommunications surveillance, the national parliaments must work on the basis of the restrictions laid down in Article 8 of the ECHR, i.e. the relevant legal rules must be necessary and proportional and their implications for individuals must be foreseeable. In addition, adequate and effective monitoring arrangements must be introduced commensurate with the powers of the intelligence agencies.

Moreover, in most states the national parliament plays an active role as the monitoring authority, given that, alongside the adoption of legislation, scrutiny of the executive, and thus also the intelligence services, is the second time-honoured function of a parliament. However, the Member State parliaments carry out this task in a very wide variety of differing ways, often on the basis of cooperation between parliamentary and non-parliamentary bodies.

9.2. The powers enjoyed by national authorities to carry out surveillance measures

As a rule, the state may carry out surveillance measures for the purposes of enforcing the law, maintaining domestic order and safeguarding national security (vis-à-vis foreign intervention)[2].

In all Member States, the principle of telecommunications secrecy may be breached for law enforcement purposes, provided that there is sufficient evidence that a crime (possibly one perpetrated under particularly aggravating circumstances) has been committed by a specific person. In view of the seriousness of the interference in the exercise of the right to privacy, a warrant is generally required for such an action[3] and the warrant then lays down precise details concerning the permissible duration of the surveillance, the relevant supervisory measures and the deletion of the collected data.

For the purposes of guaranteeing national security and order, the state's right to obtain information is extended beyond the scope of individual investigations prompted by firm

[1] See Chapter 7.
[2] Article 8(2) of the ECHR lays down these issues as grounds justifying interference in an individual's exercise of the right to privacy. See 8.3.2. above.
[3] British law is an exception, giving the Home Secretary the power to issue authorisations (Regulation of Investigatory Powers Act 2000, Section 5(1) and (3)(b)).

evidence that a crime has been committed. National law authorises the state to carry out additional measures to secure information about specific persons or groups with a view to the early detection of extremist or subversive movements, terrorism and organised crime. The relevant data is collected and analysed by specific domestic intelligence services.

Finally, a substantial proportion of surveillance measures are carried out for the purposes of safeguarding state security. As a rule, responsibility for processing, analysing and presenting relevant information about foreign individuals or countries lies with the state's own foreign intelligence service[1]. In general the surveillance targets are not specific persons, but rather set areas or radio frequencies. Depending on the resources and legal powers of the foreign intelligence service concerned, surveillance operations may cover a wide spectrum, ranging from purely military surveillance of short-wave radio transmissions to the surveillance of all foreign telecommunications links. In some Member States the surveillance of telecommunications for purely intelligence purposes is simply prohibited[2], in other Member States – in some cases subject to authorisation by an independent commission[3] - it is carried out on the basis of a ministerial order[4], possibly even without restriction in the case of some communication media[5]. The relatively broad powers enjoyed by some foreign intelligence services can be explained by the fact that their operations are targeted on the surveillance of foreign communications and thus only concern a small proportion of their own legal subjects, hence the substantially concern regarding lesser degree of misuse of their powers.

9.3. Monitoring of intelligence services

Effective and comprehensive monitoring is particularly important for two reasons: firstly, because intelligence services work in secret and on a long-term basis, so that the persons concerned often learn that they were surveillance targets only long after the event or, depending on the legal situation, not at all; and, secondly, because surveillance measures often target broad, vaguely defined groups of persons, so that the state can very quickly obtain a very large volume of personal data.

Irrespective of the form they take, all monitoring bodies naturally face the same problem: given the very nature of secret services, it is often extremely difficult to determine whether all the requisite information has in fact been provided, or whether some details are being held back. The relevant rules must therefore be framed all the more carefully. As a matter of principle, the effectiveness of the monitoring can be said to be high, and far-reaching guarantees that the interference is consistent with the law can be said to exist, if the power to order telecommunications surveillance is reserved for the highest administrative authorities, if the surveillance can be implemented only on the basis of a warrant issued by a judge and if an independent body scrutinises the performance of the surveillance measures. In addition, on

[1] For comprehensive details of the activities of foreign intelligence services, see Chapter 2.
[2] For example, in Austria and Belgium.
[3] For example, in Germany, law on the restriction of post and telecommunications secrecy (Law on Article 10 of the Basic Law). Pursuant to paragraph 9, except in cases where there is a risk that delay would frustrate the operation, the commission must be informed before the surveillance is carried out..
[4] For example in the United Kingdom (Regulation of Investigatory Powers Act, Section 1), and in France for cable communications (Law 91/646 of 10 July 1991 – loi relative au secret des correspondances émises par la voie de télécommunications).
[5] For example cable communications in France (Article 20 of Law 91/646 of 10 July 1991 - loi relative au secret des correspondances émises par la voie de télécommunications).

democratic and constitutional grounds it is desirable that the work of the intelligence service as a whole should be subject to monitoring by a parliamentary body, in accordance with the principle of the division of powers.

In Germany, these conditions have largely been met. Telecommunications surveillance measures are ordered by the responsible federal minister. Unless there is a risk that further delay may frustrate the operation, prior to the implementation of surveillance measures an independent commission not bound by government instructions (G10 Commission[1]) must be notified so that it can rule on the need for and the admissibility of the proposed measure. In those cases in which the German Federal Intelligence Service, FIS, can be authorised to carry out surveillance of non-cable telecommunications traffic with the aid of filtering on the basis of search terms, the Commission rules on the admissibility of the search terms as well. The G10 Commission is also responsible for checking that the persons under surveillance are notified, as required by the law, and that the FIS destroys the collected data.

Alongside this, there is a parliamentary monitoring body (PMB)[2], which comprises nine Members of the Bundestag and scrutinises the activities of all three German intelligence services. The PMB has the right to inspect documents, to take evidence from intelligence service staff, to visit the premises of the services and to have information notified to it; this last right can be denied only on compelling grounds concerning access to information, if it is necessary to protect the right of privacy of third parties, or if the core area of government responsibility is concerned. The proceedings of the PMB are secret and its members are required to maintain confidentiality even after they have left office. At the half-way point and at the end of the parliamentary term, the PMB submits to the German Bundestag a report on its monitoring activities.

It must be said, however, that comprehensive, almost unbroken monitoring of intelligence services is the exception in the Member States.

In France[3], for example, only those surveillance measures entailing the tapping of a cable require the authorisation of the Prime Minister. Only measures of that kind are subject to monitoring by the Commission set up for that purpose (National Commission for the Monitoring of Security-related Interceptions), whose members include an MP and a Senator. Applications for authorisation to carry out an interception operation are submitted by a minister or his or her representative to the chairman of the Commission, who, if the lawfulness of the proposed operation is in doubt, may convene a meeting of the Commission, which issues recommendations and, if there are grounds for suspecting a breach of the criminal law, informs the state prosecutor's office. Measures carried out in defence of national interests which entail the interception of radio transmissions, and thus also satellite communications, are not subject to any restrictions, including monitoring by a commission.

Moreover, the work of the French intelligence services is not subject to scrutiny by a parliamentary monitoring committee; however, moves are afoot to set up such a committee. The

[1] For full details see 'The Parliamentary Supervision of the Intelligence Services in Germany, as at 9.9.2000', published by the German Bundestag, Secretariat of the Parliamentary Control Body.
[2] Law on the supervision of federal intelligence activities (PKGrG) of 17 June 1999, BGBl I 1334 idg F.
[3] Law 91-646 of 10 July 1991; loi relative au secret des correspondances émises par la voie de télécommunications.

Defence Committee of the National Assembly has already approved such a proposal[1], but no discussion of that proposal has yet taken place in plenary.

In the United Kingdom, every communications surveillance measure carried out on British soil requires the authorisation of the Home Secretary. However, the wording of the law does not make it clear whether the non-targeted interception of communications, communications which are then checked using keywords, would also be covered by the concept of 'interception' as defined in the Regulation of Investigatory Powers Act 2000 (RIP) if the intercepted communications were not analysed on British soil, but merely transmitted abroad as 'raw material'. Checks on compliance with the provisions of the RIP are carried out on an ex-post facto basis by Commissioners – sitting or retired senior judges appointed by the Prime Minister. The Interception Commissioner monitors the granting of interception authorisations and supports investigations into complaints concerning interception measures. The Intelligence Service Commissioner monitors the authorisations granted for the activities of the intelligence and security services and supports investigations into complaints concerning those services. The Investigatory Powers Tribunal, which is chaired by a senior judge, investigates all complaints concerning interception measures and the activities of the services referred to above.

Parliamentary scrutiny is carried out by the Intelligence and Security Committee (ISC)[2], which monitors the activities of all three civilian intelligence services (MI5, MI6 and GCHQ). In particular, it is responsible for scrutinising the expenditure and administration and monitoring the activities of the security service, the intelligence service and GCHQ. The committee comprises nine members drawn from the two Houses of Parliament; ministers may not be members. Unlike the monitoring committees set up by other states, which are generally elected by the national parliament or appointed by the Speaker of that parliament, they are appointed by the Prime Minister after consulting the Leader of the Opposition.

These examples already demonstrate clearly that the level of protection varies very substantially. As far as parliamentary scrutiny is concerned, your rapporteur would like to point out that the existence of a monitoring committee responsible for scrutinising the activities of intelligence services is very important: in contrast to the normal parliamentary committees, they have the advantage of enjoying a higher degree of trust among the intelligence services, given that their members are bound by the confidentiality rule and committee meetings are held in camera. In addition, with a view to the performance of their special task they are endowed with special rights vital to the monitoring of activities in the intelligence sector.

Your rapporteur is pleased to report that most of the EU Member States have set up a separate parliamentary monitoring committee to scrutinise the activities of the intelligence services. In Belgium[3], Denmark[4], Germany[5], Italy[1], the Netherlands[2] and Portugal[3], there is a parliamentary

[1] See the Bill entitled 'Proposition de loi tendant á la création de délégations parlementaires pour le renseignement', and the related report by Mr Arthur Paecht, No 1951, National Assembly, 11th parliamentary term, registered on 23 November 1999.
[2] Intelligence Services Act 1994, Section 10.
[3] Comité permanent de côntrole des services de renseignements et de sécurité, Comité permanent R, Loi du 18 juillet 1991 / IV, organique du contrôle des services de police et de renseignements.
[4] Udvalget vedrorende efterretningstjenesterne, Lov Ombudsman etablering af et udvalg Ombudsman forsvarets og politiets efterretningsjenester, lov 378 af 6.7.88.
[5] Das parlamentarische Kontrollgremium (PKGr), Gesetz über die Kontrolle nacrhichtendienstlicher Tätigkeit des Bundes (PKGrG) vom 17 Juni 1999 BGB1 I 1334 idgF.

monitoring committee responsible for scrutinising both the military and civilian intelligence service. In the United Kingdom[4] the special monitoring committee scrutinises only the admittedly much more significant activities of the civilian intelligence services; the military intelligence service is monitored by the normal defence committee. In Austria[5] the two arms of the intelligence service are dealt with by two separate monitoring committees, which are, however, organised in the same way and endowed with the same rights. In the Nordic states Finland[6] and Sweden[7] parliamentary scrutiny is carried out by Ombudsmen, who are independent and elected by parliament. France, Greece, Ireland, Luxembourg and Spain have no special parliamentary committees; in these countries, monitoring tasks are carried out by the standing committees as part of their general parliamentary work.

9.4. Assessment of the situation for European citizens

The situation for European citizens in Europe is unsatisfactory. The powers of national intelligence services in the sphere of telecommunications surveillance differ very substantially in scope, and the same applies to the powers of the monitoring committees. Not all those Member States which operate an intelligence service have also set up independent parliamentary monitoring bodies endowed with the appropriate supervisory powers. A uniform level of protection is still a distant objective.

From a European point of view, this is all the more regrettable, because this state of affairs does not primarily affect the citizens of the Member States concerned, who can influence the level of protection by means of their voting behaviour in elections. The adverse impact is felt above all by nationals of other states, since foreign intelligence services, by their very nature, carry out their work abroad. Individuals are essentially at the mercy of foreign systems, and here the need for protection is greater still. It must also be borne in mind that, by virtue of the specific nature of intelligence services, EU citizens may be affected by the activities of several such services at the same time. In this context, a uniform level of protection consistent with democratic principles would be desirable. Consideration should also be given to the issue of whether data protection provisions in this sphere would be workable at EU level.

Moreover, the issue of the protection of European citizens will be placed in an entirely new context when, under a common security policy, the first moves are made towards cooperation among the Member States' intelligence services. Citizens will then look to the European

---

[1] Comitato parlamentare, L. 24 ottobre 1977, n. 801, art. 11, Istituzione e ordinamento de servizi per le informazioni e la sicurezza e disciplina del segreto di Stato.

[2] Tweede-Kamercommissie voor de Inlichtingen-en Veiligheidsdiensten, 17. Reglement van order van de Tweede Kamer der Staten-General, Art. 22.

[3] Conselho de Fiscalizações (CFSI), Law 30/84 of 5.9.1984, amended by Law 4/95 of 21.2.1995, Law 15/96 of 30.4.1996 and Law 75-A/97 of 22.7.1997.

[4] Intelligence and Security Committee (ISC), Intelligence Services Act 1994, Section 10.

[5] Standing Subcommittee of the National Defence Committee responsible for monitoring intelligence measures to safeguard military security and the Standing Subcommittee of the Committee on Internal Affairs responsible for monitoring measures to protect constitutional bodies and their ability to act, Article 52a B-VG, §§ 32b et seq., Law on the Rules of Procedure, 1975.

[6] Ombudsman, legal basis for supervision of the police (SUPO): Poliisilaki 493/1995 § 33 and Laki pakkokeinolain 5 a luvun muuttamisesta 366/1999 § 15, for the military: Poliisilaki 493/1995 § 33 and Laki poliisin tehtävien suorittamisesta puolustusvoimissa 1251/1995 § 5.

[7] Rikspolisstyrelsens ledning, Förordning (1998: 773) med instruktion för Rikspolisstyrelsen (Regulation (1989: 773) on the national police authority).

institutions to adopt adequate protection provisions. The European Parliament, as an advocate of constitutional principles, will then have the task of lobbying for the powers it needs, as a democratically elected body, to carry out appropriate monitoring. In this connection, the European Parliament will also be required to establish conditions under which the confidential processing of sensitive data of this kind and other secret documents by a special committee whose members are bound by a duty of discretion can be guaranteed. Only once these conditions have been met will it be realistic, and, with a view to effective cooperation among intelligence services – the *sine qua non* of a serious common security policy – responsible, to press for these monitoring rights.

10. Protection against industrial espionage

10.1. Firms as espionage targets

The information held by firms falls into three categories as far as the need for secrecy is concerned. Firstly, there is information which is deliberately **disseminated as widely as possible**. This includes technical information about a firm's products (e.g. specifications, prices, etc.) and promotional information which has a bearing on a firm's image.

Secondly, there is information which is **neither protected nor actively disseminated**, because it has no bearing on a firm's competitive position. Examples includes the date of the works outing, the menu in the works canteen or the make of fax machine used by a firm.

Finally, there is information which is **protected against third parties**. The information is protected against competitors, but also, if a firm intends to break the law (tax provisions, embargo rules, etc.), against the state. There are various degrees of protection, culminating in strict secrecy, e.g. in the case of research findings prior to the registration of a patent or armaments production[1].

In the case under discussion here, espionage involves obtaining information kept secret by a firm. If the assailant is a rival firm, the term used is **competitive intelligence**. If the assailant is a state intelligence service, the relevant term is **industrial espionage**.

10.1.1. Espionage targets in detail

Strategic information relevant to espionage against firms can be classified according to sectors of the economy or the departments of individual firms.

10.1.1.1. Sectors of the economy

It is perfectly obvious that information in the following sectors is of particular interest: biotechnology, genetic technology, medical technology, environmental technology, high-performance computers, software, optoelectronics, image sensing and signalling systems, data storage systems, industrial ceramics, high-performance alloys and nanotechnology. The list is not comprehensive and changes constantly in line with technological developments. In these sectors of industry, espionage primarily involves stealing research findings or details of special production techniques.

10.1.1.2. Departments of individual firms

The following departments are logical espionage targets: research and development, procurement, personnel, production, distribution, sales, marketing, product lines and finance. The significance and value of such information is often underestimated (see 10.1.14).

[1] Information for firms provided with security protection, BMWI 1997.

10.1.2. Competitive intelligence

The strategic position of a firm on the market depends on its capabilities in the following spheres: research and development, production procedures, product lines, funding, marketing, sales, distribution, procurement and personnel[1]. Information on these capabilities is of major interest to any of the firm's competitors, since it gives an insight into the firm's plans and weaknesses and enables rivals to take strategic countermeasures.

Some of this information is publicly available. There are highly specialised consultancies, including such respected firms as Roland & Berger in Germany, which draw up, on an entirely legal basis, analyses of the competitive position on a given market. In the USA competitive intelligence has now become a standard management tool[2]. Professional analysis can turn a wide range of individual items of information into a clear picture of the situation as a whole.

The transition from legality to a criminal act of competitive intelligence is bound up with the choice of means used to obtain information. Only if the means employed are illegal under the laws of the country concerned do efforts to obtain information become a criminal act – the provision of analyses is not in itself punishable under the law. Naturally enough, information of particular interest to competitors is protected and can only be obtained by criminal means. The techniques employed for this purpose are in no way different from the general espionage methods described in Chapter 2.

No precise details are available concerning the scale of competitive intelligence operations. As in the case of conventional espionage, the official figures represent only the tip of the iceberg. Both parties concerned (perpetrator and victim) are keen to avoid publicity. Espionage is always damaging to the image of the firms concerned and the assailants naturally have no interest in public light being shed on their activities. For that reason, very few cases come to court.

Nevertheless, reports dealing with competitive intelligence repeatedly appear in the press. In addition, your rapporteur has discussed this issue with the heads of security of a number of large German firms[3] and with managers of American and European firms. The conclusion to be drawn is that cases of competitive intelligence repeatedly come to light, but do not determine firms' day-to-day behaviour.

10.2. Damage caused by industrial espionage

In view of the high number of unrecorded cases, it is difficult to determine precisely the extent of the damage caused by competitive intelligence/industrial espionage. In addition, some of the figures quoted are inflated because of vested interests. Security firms and counter-intelligence services have an understandable interest in putting the losses at the high end of the realistically possible scale. Despite this, the figures do give some idea of the problem.

As early as 1988, the Max Plank Institute estimated that the damage caused by industrial espionage in Germany amounted to at least DM 8 billion[4]. The chairman of the association of

[1] M.F. Porter, Competitive Strategy.
[2] Roman Hummelt, Industrial espionage on the data highway, Hanserverlag, Munich, 1997.
[3] Details and names confidential.
[4] Impulse, 3797, p. 13 et seq.

security consultants in Germany quotes a figure of DM 15 bn a year, based on expert evidence. The President of the European police trade unions, Hermann Lutz, puts the damage at DM 20 bn a year. According to the FBI[1], US industry suffered losses of US$ 1.7 bn as a result of competitive intelligence and industrial espionage in the years 1992/1993. The former chairman of the Secret Service monitoring committee of the House of Representatives in the USA has spoken of losses of US $100 bn sustained through lost contracts and additional research and development costs. It is claimed that between 1990 and 1996 this resulted in the loss of 6 million jobs[2].

Basically the exact scale of the losses is irrelevant. The state has an obligation to combat competitive intelligence and industrial espionage using the police and counter-intelligence services, irrespective of the level of damage to the economy. Similarly, decisions taken by firms on the protection of information and counter-espionage measures cannot be based on total damage figures. Every firm has to calculate for itself the maximum possible damage as a result of the theft of information, assess the likelihood of such events occurring and compare the potential losses with the costs of security. The real problem is not the lack of accurate figures for the overall losses, the position is rather that such cost/benefit calculations are rarely carried out, except in large firms, and consequently security is disregarded.

10.3. Who carries out espionage?

According to a study by the auditors Ernest Young LLP[3], 39% of industrial espionage is carried out on behalf of competitors, 19% for clients, 9% for suppliers and 7% for secret services. Espionage is carried out by company employees, private espionage firms, paid hackers and secret service professionals[4].

10.3.1. Company employees (insider crime)

According to the literature examined, the expert evidence presented to the committee and the rapporteur's discussions with heads of security and counter-espionage authorities, there is a consensus that the greatest risk of espionage arises from disappointed and dissatisfied employees. As employees of the firm, they have direct access to information, can be recruited for money and will spy on their employer to obtain industrial secrets for those who hire them.

Major risks also arise when employees change jobs. Today it is not necessary to copy mountains of paper in order to take important information out of the firm. Such information can be stored on diskettes unnoticed and taken to the new employer when employees change job.

10.3.2. Private espionage firms

The number of firms specialising in espionage is on the increase. Former members of the intelligence services sometimes work in these firms. Frequently the firms concerned also operate as security consultants and as detective agencies employed to obtain information. In general, the methods used are legal but there are also firms which employ illegal means.

[1] Congressional statement, L. J. Freeh, FBI Director, 9.5.1996.
[2] Robert Lyle, Radio Liberty/Radio Free Europe, 10.2.1999.
[3] Computerzeitung, 30.11.1995, p. 2.
[4] R. Hummelt, Spionage auf dem Datenhighway, Munich, 1997, p. 49 et seq.

10.3.3. Hackers

Hackers are computer specialists with the knowledge to gain access to computer networks from the outside. In the early days, hackers were computer freaks who got a kick out of breaking through the security devices of computer systems. Nowadays there are contract hackers in both the services and on the market.

10.3.4. Intelligence services

Since the end of the Cold War, the focus of the intelligence services' work has shifted. International organised crime and economic data are among their new tasks (for further details see Chapter 10.5).

10.4. How is espionage carried out?

According to information provided by the counter-intelligence authorities and by the heads of security of large firms, all tried and tested intelligence service methods and instruments are used for the purposes of industrial espionage (see Chapter 2.4). Firms have a more open structure than military and intelligence service facilities or government entities. In connection with industrial espionage, they are therefore exposed to additional risks:

- the recruitment of employees is simpler, as the facilities available to industrial security services cannot be compared to those of the counter-intelligence authorities;

- workplace mobility means that important information can be taken around on a laptop. The theft of laptops or the secret copying of hard disks after hotel room break-ins is thus one of the standard methods of industrial espionage;

- it is easier to break into firm's computer networks than those of security-sensitive State bodies, as small and medium-sized firms in particular have much less developed security awareness and security precautions;

- local tapping of communications (see Chapter 3.2) is also easier for the same reasons.

Evaluation of the information gathered on this matter shows that industrial espionage is mainly carried out locally or through mobile workstations, as with a few exceptions (see Chapter 10.6) the information sought cannot be obtained by intercepting international telecommunications networks.

10.5. Industrial espionage by states

10.5.1. Strategic industrial espionage by the intelligence services

After the end of the Cold War, intelligence service capacity was released and it can now be used in other areas. The United States readily admits that some of its intelligence service's activities also concern industry. This includes, for example, monitoring of the observance of economic sanctions, compliance with rules on the supply of weapons and dual-use goods, developments on

commodities markets and events on the international financial markets. The rapporteur's findings are that the US services are not alone in their involvement in these spheres, nor is there any serious criticism of this.

10.5.2. Intelligence services as agents of competitive intelligence

Criticism is levelled when state intelligence services are misused to put firms within their territory at an advantage in international competition through espionage. A distinction has to be made here between two cases[1].

10.5.2.1. High-tech states

Highly-developed industrial states can indeed gain advantage from industrial espionage. By spying on the stage of development reached in a specific sector, it is possible to take foreign trade and subsidy measures either to make domestic industry more competitive or to save subsidies. Another focus of such activities may be efforts to obtain details of particularly valuable contracts (see 10.6).

10.5.2.2. Technologically less-advanced states

Some of these states are concerned to acquire technological know-how to enable their own industry to catch up without incurring development costs and licence fees. The aim may also be to acquire product designs and production methods in order to be able to compete on the world market with copies produced more cheaply by virtue of lower wages. There is evidence that the Russian intelligence services have been instructed to carry out such tasks. The Russian Federation's law No 5 on foreign intelligence specifically mentions obtaining industrial and scientific/technical information as one of the intelligence service's tasks.

Another group of states (for example Iran, Iraq, Syria, Libya, North Korea, India and Pakistan) are concerned to acquire information for their national arms programmes, particularly in the nuclear sector and in the area of biological and chemical weapons. A further aspect of the activities of the services of these states is the operation of front companies which can purchase dual-use goods without raising suspicion.

10.6. Is ECHELON suitable for industrial espionage?

The strategic monitoring of international telecommunications, can produce useful information for industrial espionage purposes, but only by chance. In fact, sensitive industrial information is primarily to be found in the firms themselves, which means that **industrial espionage is carried out primarily by attempting to obtain the information via employees** or infiltrators or by breaking into internal computer networks. Only where sensitive data is sent outside via cable or radio (satellite) can a communications surveillance system be used for industrial espionage. This occurs systematically in the following three cases:

- in connection with firms which operate in three times zones, so that interim results are sent from Europe to America and then on to Asia;

[1] Confidential statement to the rapporteur by a counter-intelligence service, source protected.

- in the case of videoconferences in multinational companies conducted by VSAT or cable;

- when important contracts have to be negotiated locally (construction of facilities, telecommunications infrastructure, rebuilding of transport systems, etc.), and the firm's representatives have to consult their head office.

If firms fail to protect their communications in such cases, interception can provide competitors with valuable data.

10.7. Published cases

There are some cases of industrial espionage and/or competitive intelligence which have been described in the press or in the relevant literature. Some of these sources have been analysed and the results are summarised in the following table. Brief details are given of the persons involved, when the cases occurred, the detailed issues at stake, the objectives and the consequences.

It is noticeable that sometimes a single case is reported in very different ways. One example is the Enercom case, in connection with which either the NSA, or the US Department of Commerce or the competitor which took the photographs is described as the 'perpetrator'.

Case	Who	When	What	How	Aim	Consequences	Source
Air France	DGSE	Until 1994	Conversations between travelling businessmen	Bugs were discovered in the first class cabins of Air France aircraft - public apology by the company	Obtaining information	Not stated	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
Airbus	NSA	1994	Information on an order for aircraft concluded between Airbus and the Saudi Arabian national airline	Interception of faxes and telephone calls between the negotiating parties	Forwarding of information to Airbus's American competitors, Boeing and McDonnell-Douglas	The Americans won the contract (US$ 6 bn)	„Antennen gedreht“, Wirtschaftswoche Nr.46 / 9 November 2000
Airbus	NSA	1994	Contract with Saudi Arabia worth US$ 6 bn uncovering of bribes paid by the European Airbus Consortium	Interception of faxes and telephone calls, routed via telecommunications satellites, between Airbus Consortium and the Saudi Arabian national airline/Government	Uncovering of bribes	McDonnel-Douglas, Airbus's American competitor, won the contract	“Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5 10 1999 STOA, von Duncan Campbell
BASF	Marketing manager	Not stated	Description of the process for the production of a raw material for skin creams by BASF (cosmetics division)	Not stated	Not stated	None, because the attempt was discovered	„Nicht gerade zimperlich“, Wirtschaftswoche Nr.43 / 16 October 1992
Federal German Ministry of Economic Affairs	CIA	1997	Information concerning high-tech products held by the Federal Ministry for Economic Affairs	Use of an agent	Obtaining information	Agent unmasked and expelled from the country	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
Federal German Ministry of Economic Affairs	CIA	1997	Background to the Mykonos trial in Berlin, Hermes loans concerning exports to Iran, setting-up of German firms supplying high-tech products to Iran	CIA agent disguised as US Ambassador holds friendly conversations with the Head of the Department in the Federal Ministry for Economic Affairs responsible for the Arab region (particular responsibility: Iran)	Obtaining information	Not stated Civil servant contacts the German security authorities, who inform the Americans that the CIA operation is unwelcome. CIA agent then 'withdrawn'.	Industrial espionage. Firms as a target for foreign intelligence services, Baden-Württemberg Constitutional Protection Agency, Stuttgart as at 1998
Dasa	Russian Intelligence Service	1996 – 1999	Purchase and forwarding of armaments-related documents drawn up by a Munich arms firm (according to SZ of 30.05.2000: arms firm Dasa in Ottobrunn)	2 Germans working on behalf of the Russians	Obtaining information on guided missiles, armaments systems (anti-tank and anti-aircraft missiles)	SZ / 30.05.2000: '(...) Betrayal of secrets 'not particularly serious' from a military point of view. The court ruled that this also applied to the economic damage suffered.'	„Anmerkungen zur Sicherheitslage der deutschen Wirtschaft“, ASW; Bonn, April 2001 „Haftstrafe wegen Spionage für Russland“, SZ / 30 May 2000
Embargo	FIS	Around 1990	Resumption of exports of embargoed technology to Libya (e.g. by Siemens)	Interception of telephone calls	Uncovering illegal arms and technology transfer	No particular consequences, deliveries not prevented	"Maulwürfe in Nadelstreifen", Andreas Förster, p. 110

Case	Who	When	What	How	Aim	Consequences	Source
Enercon	Wind power expert from Oldenburg and Kenetech employee	Not stated	Wind-power plant developed by Enercon, a firm located in Aurich	Not stated	Not stated	Not stated	„Anmerkungen zur Sicherheitslage der deutschen Wirtschaft“, ASW; Bonn, April 2001
Enercon	NSA	Not stated	Wind wheel for electricity generation, developed by Aloys Wobben, an engineer from East Frisia	Not stated	Forwarding of technical details of Wobben's wind wheel to a US firm	US firm patents the wind wheel before Wobben; Wobben taken to court by US lawyers (breach of patent rights)	„Aktenkrieger“, SZ, 29 March 2001
Enercon	US firm Kenetech Windpower Corp	1994	Important details of a high-tech wind-powered electricity generating plant (from switch gears to sails)	Photographs	Successful patent application in the USA	Enercon abandons its plans to attack the US market	„Sicherheit muss künftig zur Chefsache werden“, HB / 29 August 1996
Enercon	Engineer W., from Oldenburg, and US firm Kenetech	March 1994	Type E-40 wind-powered electricity generator developed by Enercon	Engineer W. passes on details, Kenetech employee photographs the plant and electrical components	Kenetech: seeking evidence for subsequent (1995) legal action against Enercon for breach of patent rights Enercon: industrial espionage Television journalist claims to have learned from a former NSA employee that detailed information about Enercon was obtained using Echelon and passed on to Kenetech by the Americans	Not stated	„Klettern für die Konkurrenz“, SZ 13 October 2000
Enercon	Kenetech Windpower	Before 1996	Data concerning Enercon's wind-powered electricity generating plant	Kenetech engineers photograph the plant	Kenetech copies the plant	Enercon vindicated; legal action brought against spy; estimated loss: several hundred million DM	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
Japanese Trade Ministry	CIA	1996	Negotiations on import quotas for US cars on the Japanese market	Hacking into computer system of the Japanese Trade Ministry	US negotiator Mickey Kantor should accept lowers offer	Kantor accepts lowest offer	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
Japanese cars	US Government	Not stated	Negotiations on the import of Japanese luxury cars Information on the emissions standards of Japanese cars	COMINT, no detailed information	Obtaining information	No details	“Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5 10 1999 STOA, by Duncan Campbell

Case	Who	When	What	How	Aim	Consequences	Source
López	NSA	Not stated	Videoconference involving VW and López	Interception from Bad Aibling	Forwarding of information to General Motors and Opel	The interception operation allegedly provided the State Prosecutor's Office with 'very detailed evidence' for its investigation	Bundeswehr Captain Erich Schmidt-Eenboom, quoted in 'Wenn Freunde spionieren' www.zdf.msnbc.de/news/54637.asp?cp1=1
López	López and three of his staff	1992 - 1993	Papers and information concerning research, planning, manufacturing and purchasing (documents concerning a plant in Spain, cost information for various model ranges, project studies, purchasing and saving strategies)	Collecting information	Use of General Motors documents by VW	In the wake of legal action, the firms settle out of court. In 1996, López resigns as VW manager, in 1997 VW dismisses three further members of the López team, pays US$ 100 m to GM/Opel (supposedly lawyers' fees) and over a seven-year period purchases spare parts from GM/Opel for a total of US$ 1 billion.	Industrial espionage. Firms as a target for foreign intelligence services, Baden-Württemberg Constitutional Protection Agency, Stuttgart as at 1998
López	NSA	1993	Videoconference between José Ignacio López and VW boss Ferdinand Piëch	Videoconference recorded and forwarded to General Motors (GM)	Protection of commercial secrets held by GM in America, secrets which López wished to pass on to VW (price lists, secret plans for a new car plant and a new small car)	López's cover is blown, in 1998 criminal proceedings are halted in return for payment of fines. No consequences in respect of NSA	„Antennen gedreht“, Wirtschaftswoche Nr.46 / 9 November 2000 „Abgehört“, Berliner Zeitung, 22 January 1996 „Die Affäre López ist beendet“, Wirtschaftsspiegel, 28 July 1998 „Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
Los Alamos	Israel	1988	Two employees of the Israeli nuclear research programme hack into the central computer of the Los Alamos nuclear weapons laboratory	Hacking	Obtaining information about new fuses for US atomic weapons	No specific consequences, since the hackers fled to Israel. One is briefly held in custody in Israel, links with the Israeli Secret Service are not officially confirmed	"Maulwürfe in Nadelstreifen", Andreas Förster, p. 137
Smuggling	FIS	1970s	Smuggling of computers into the GDR	Not stated	Uncovering of technology transfer to the Eastern Bloc	No particular consequences, deliveries not prevented	"Maulwürfe in Nadelstreifen", Andreas Förster, p. 113

Case	Who	When	What	How	Aim	Consequences	Source
TGV	DGSE	1993	Cost calculation by Siemens Contract to supply high-speed trains to South Korea	Not stated	Lower price offer	The manufacturer of the ICE loses the contract to Alcatel-Alsthom	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
TGV	Unknown	1993	Cost calculation by AEG and Siemens concerning a government contract to supply South Korea with high-speed trains	Siemens claims that the telephone and fax connections in its Seoul office are being tapped	Negotiating advantage for the Anglo-French competitor GEC Alsthom	South Korea decides in favour of GEC Alsthom, although the German offer was initially regarded as better	„Abgehört“, Berliner Zeitung, 22 January 1996
Thomson-Alcatel v Raytheon	CIA/ NSA	1994	Award to the French firm Thomson-Alcatel of a Brazilian contract for the satellite monitoring of the Amazon Basin (US$ 1.4 bn)	Interception of communications to and from the successful tenderer (Thomson-Alcatel)	Uncovering corruption (payment of bribes)	Clinton complains to the Brazilian Government; under pressure from the US Government, the contract is awarded to the US firm Raytheon	"Maulwürfe in Nadelstreifen", Andreas Förster, p. 91
Thomson-Alcatel v Raytheon	US Department of Commerce 'made efforts'	1994	Negotiations on a project worth billions of dollars concerning the radar monitoring of the Brazilian rainforest	Not stated	Win contract	The French firms Thomson CSF and Alcatel lose the contract to the US firm Raytheon	„Antennen gedreht“, Wirtschaftswoche Nr.46 / 9 November 2000
Thomson-Alcatel v Raytheon	NSA Department of Commerce		Negotiations concerning a project worth US$ 1.4 bn concerning the monitoring of Amazon Basin (SIVA) Discovery that the Brazilian selection panel had accepted bribes. Comment by Campbell: Raytheon supplies equipment for the Sugar Grove interception station	Surveillance of the negotiations between Thomson-CSF and Brazil and forwarding of the findings to Raytheon Corp.	Uncovering bribery Winning of the contract	Raytheon wins the contract	“Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5 10 1999 STOA, von Duncan Campbell http://www:raytheon:com/sivam/contract:html
Thyssen	BP	1990	Gas and oil drilling contract in the North Sea worth millions of dollars	Interception of faxes sent by the successful tenderer (Thyssen)	Uncovering corruption	BP brings an action for damages against Thyssen	"Maulwürfe in Nadelstreifen", Andreas Förster, p. 92
VW	Unknown	'recent years'	Not stated	Inter alia, infrared camera, fixed in a mound of earth, which transmits images by radio	Obtaining information about new developments	VW admits losses of profits totalling hundreds of millions of deutschmarks	„Sicherheit muss künftig zur Chefsache werden“, HB / 29 August 1996

VW	Unknown	1996	VW test circuit in Ehra-Lessien	Hidden camera	Information about new VW models	Not stated	„Auf Schritt und Tritt“ Wirtschaftswoche Nr. 25, 11 June 1998

10.8. Protection against industrial espionage

10.8.1. Legal protection

The legal systems of all the industrialised countries define the theft of commercial secrets as a criminal offence. As in all other areas of the criminal law, the degree of protection varies from country to country. As a rule, however, the penalties for industrial espionage are much less severe than those for espionage in connection with military security. In many cases, competitive intelligence operations are banned only against firms from the same country, but not against foreign firms abroad. This is also the case in the USA.

In essence, the relevant laws prohibit only espionage by one industrial undertaking against another. It is doubtful whether they also restrict the activities of state intelligence services, since, on the basis of the laws establishing them, the latter are authorised to steal information.

A grey area develops if intelligence services seek to pass on to individual firms information gained by means of espionage. The laws which endow intelligence services with special powers would normally not cover such activities. In particular, in the EU this would represent a breach of the EEC Treaty (see Chapter …).

Irrespective of this fact, however, in practice it would be very difficult for a firm to seek legal protection by bringing an action before the courts. Interception operations leave no trace and generate no evidence which might be used in court.

10.8.2. Other obstacles to industrial espionage

States accept the fact that intelligence services, in keeping with their general objective of securing strategic information, are also active in the commercial sphere. However, this gentlemen's agreement is frequently breached in connection with competitive intelligence operations designed to benefit a country's own industry. Any state caught red-handed comes under massive political pressure. This applies in particular to a world power such as the USA, whose claim to global political leadership would be drastically undermined. Middle-ranking powers could probably afford to be singled out for such activities; a superpower certainly cannot.

Alongside the political problems, there is also the practical issue of which individual firm is to be provided with the information gained by means of competitive intelligence operations. In the aerospace sector, the answer is a simple one, because the global market is dominated by only two major firms. In all other cases where a market is supplied by a number of firms which are not state-controlled, it is extremely difficult to give preference only to one. In connection with international contract-award procedures, an intelligence service is more likely to forward detailed information concerning other competitors' offers to all the participating firms from its own country, rather than simply to one. This applies in particular when all the participating firms from one country can draw on the same level of government support, as is the case in the USA through the work of the Advocacy Center. In the case of the theft of technology, which should necessarily lead to the registration of a patent, it is only logical that such equal treatment would no longer be possible.

Moreover, under the American political system in particular this would give rise to a serious problem. American politicians are massively dependent on contributions from firms in their constituencies to finance their election campaigns. If proof were to emerge of even one case of intelligence services favouring individual firms, the upheaval in the political system would be massive. As the former CIA Director James Woolsey put it in a discussion with representatives of the committee: 'In that case the Hill (i.e. the US Congress) would go mad!'. Quite!

10.9. The USA and industrial espionage

10.9.1. The official US position on industrial espionage

The position adopted by the former CIA Director James Woolsey and the chairman of the House of Representatives Secret Service Monitoring Committee, Porter Goss, in our discussions can be summarised as follows:

1. The USA monitors international telecommunications in order to obtain general information about economic developments, shipments of dual-use goods and compliance with embargoes.

2. The USA monitors on a targeted basis communications by individual firms in connection with contract-award procedures in order to prevent corruption-related distortions of competition to the detriment of US firms.

American firms are banned by law from paying bribes and accountants are required to report evidence of such payments. If a telecommunications surveillance operation reveals evidence of bribery in connection with public contracts, the US ambassador makes representations to the government of the country concerned. However, US firms competing for the contract are not directly informed.

10.9.2. The role of the Advocacy Center in promoting US exports

10.9.2.1. The task of the Advocacy Center

The Advocacy Center, which is attached to the US Department of Commerce, is at the heart of the national export strategy employed by President Clinton and continued by President Bush. Since its inception in 1993 the Center has helped hundreds of US firms to win public contracts abroad. The Center focuses the resources of the US Administration, ranging from experts in individual sectors, via the economic attachés posted to embassies, right up to the White House.

10.9.2.2. The Advocacy Center's operating methods

The Center itself has only a small staff complement of 12 persons (as at 6 February 2001). It provides firms with a central contact point for their dealings with the various US authorities involved in promoting exports. It works on behalf of firms on a non-discriminatory basis, but, in line with the clear rules governing its work, supports only projects which are in the US

national interest. For example, products manufactured in the USA must make up at least 50% of the value of the goods delivered under any given contract.

10.9.2.3. Open questions in connection with the Advocacy Center

The US Administration did not allow the planned discussion between members of the committee and representatives of the Center to take place. For that reason, two areas of doubt could not be cleared up:

a. the committee has in its possession documents which seem to provide evidence of CIA involvement in the work of the Center;

b. on the basis of information placed on the Internet, the Center acknowledges that it focuses the resources of 19 'US government agencies'. Elsewhere, however, only 14 such agencies are listed, raising the issue of why five agencies cannot be named in public.

10.10. Security of computer networks

to follow

10.11. Under-estimation of the risks

to follow

10.11.1. Large firms

10.11.2. Small and medium-sized businesses

10.11.3. European institutions

10.11.4. Research bodies

11. Cryptography as a means of self-protection

11.1. Purpose and method of encryption

11.1.1. Purpose of encryption

Every time a message is transmitted, there is a risk of its falling into unauthorised hands. To prevent outsiders ascertaining its content in such cases, the message must be made impossible for them to read or intercept, i.e. encrypted. Consequently encryption techniques have been used since time immemorial for military and diplomatic purposes[1].

In the past 20 years the importance of encryption has increased, since an ever greater proportion of communications has been sent abroad, where the confidentiality of post and telecommunications could not be guaranteed by the state of origin. Moreover, the expanded technical opportunities for the state legally to intercept/record communications on its own territory has led to concern among ordinary citizens and a greater need for their protection. Finally, the increased interest among criminals in having illegal access to information, and the ability to falsify it, has also given rise to protection measures (e.g. in the banking sector).

The invention of electrical and electronic communications (telegraph, telephone, radio, telex, fax and Internet) greatly simplified the transmission of intelligence communications and made them immeasurably quicker. The downside was that there was no **technical** protection against interception or recording, so that anyone with the right equipment could read the communication if he could gain access to the means of communication. If done professionally, interception leaves little or no trace. This imparted a new significance to encryption. It was the banking sector which first regularly used encryption to protect communications in the new area of electronic money transfers. The growing internationalisation of the economy led to communications in this field, too, being at least partly protected by cryptography. The widespread introduction of completely unprotected communications through the Internet also increased the need for private individuals to protect their messages from interception.

In the context of this report, then, the question arises as to whether there are cheap, legal, sufficiently secure and user-friendly methods of encrypting communications which can protect the individual against interception.

11.1.2. How encryption works

The principle of encryption is to convert a plain text into an encrypted text in such a way that it has either no meaning or a different meaning from the original, but can be converted back to the original by those in the know. For example, a meaningful sequence of letters can be transformed into a meaningless sequence which no outsider understands.

This is done according to a given method (encryption algorithm) based on the transposition and/or the substitution of letters. **The encryption method** (algorithm) is not nowadays kept

[1] There is evidence of this even in antiquity, e.g. the use of the *skytale* or cipher rod by the Spartans in the 5th century BC.

secret. On the contrary, a worldwide invitation to tender was recently issued for a new global encryption standard for use in industry. The same was done for the creation of a specific encryption algorithm as hardware in a machine (e.g. an encrypted fax machine).

What is **really secret** is the **key to the code.** This can be best explained by analogy. It is generally public knowledge how door locks work, not least because patents are held on them. Individual doors are protected by the fact that several different keys can exist for a particular type of lock. The same goes for the encryption of information: **many different** messages may be protected using individual keys, **kept secret** by those involved, on the basis of **one publicly known encryption method** (algorithm).

To explain these terms, we may use the example of the 'Caesarean encryption'. Julius Caesar encrypted messages simply by replacing each letter with the letter three places further on in the alphabet (A became D, B became E, etc.). The word **ECHELON** would thus become **HFKHORQ.** The **encryption algorithm** thus consists of the **shifting of letters** within the alphabet, and the **key** in this particular case is the instruction to move the letters **three places in the alphabet.** Both encryption and decryption are done in the same way: by moving letters three places: a symmetrical process. Nowadays this type of process would not provide protection for as much as a second!

A good encryption system may perfectly well be publicly known and still be regarded as secure. For this purpose, however, the number of possible keys needs to be so large that it is not possible to try all the keys (known as a **brute force attack**) in a reasonable time, even using computers. However, a large number of possible keys does not necessarily imply secure encryption if the method results in an encrypted text which gives clues to its decryption (e.g. the frequency of particular letters)[1]. Caesarean encryption is thus an insecure system for both reasons. Because it uses simple substitution, the varying frequency of letters in a language means that the procedure can quickly be cracked; moreover, since there are only 26 letters in the alphabet, there are only 25 possible letter shifts and thus only 25 possible keys. In this case, then, the codebreaker could very quickly find the key by trying all the possibilities and decipher the text.

We will now consider what a secure system should look like.

11.2. Security of encryption systems

11.2.1. Meaning of 'security' in encryption: general observations

If an encryption system is required to be 'secure', this may mean one of two things. Either it may be essential – and susceptible of mathematical proof – that the message is impossible to decipher without the key. Or it may be sufficient for the code to be unbreakable at the present state of technology and thus in all probability to meet the security requirement for far longer than the 'critical' period during which the message needs to be kept secret.

[1] cf. Leiberich, 'Vom diplomatischen Code zur Falltürfunktion – Hundert Jahre Kryptographie in Deutschland' [From diplomatic code to trap-door function – a hundred years of cryptography in Germany], *Spektrum der Wissenschaft* June 1999, p. 26 et seq.

11.2.2. Absolute security: the one-time pad

At present the only absolutely secure method is the one-time pad. This system was developed towards the end of the First World War[1], but was also used later for the telex hot-line between Moscow and Washington. The concept consists of a key comprising a non-repeating row of completely random letters. Both sender and recipient encrypt using these rows, and destroy the key as soon as it has been used once. Since there is no internal order within the key, it is impossible for a cryptoanalyst to break the code. This can be mathematically proven.[2]

The drawback to this process is that it is not easy to generate large numbers of these random keys[3], and that it is difficult and impractical to find a secure means of distributing the key. In normal business transactions, therefore, this method is not used.

11.2.3. Relative security at the present state of technology

11.2.3.1. The use of decryption and encryption machines

Even before the invention of the one-time pad, cryptographic processes were developed which could generate a large number of keys and thus produce coded texts which contained as few regularities in the text as possible and thus few starting-points for codebreaking. In order to make these methods sufficiently fast for practical application, machines were developed for encryption and decryption. The most spectacular of these was probably Enigma[4], used by Germany in the Second World War. The small army of decryption experts working at Bletchley Park in England succeeded in cracking the Enigma code by means of special machines known as 'bombs'. Both the Enigma machine and the 'bombs' were mechanical in operation.

11.2.3.2. Use of computers in cryptography

The invention of the computer represented a breakthrough in cryptography, since its power made it possible to use increasingly complex systems. Even though it did not alter the basic principles of encryption, a number of changes took place. Firstly, the level of potential complexity of the encryption system was multiplied, since it was no longer subject to the constraints of what was mechanically feasible, and, secondly, the speed of the encryption process rose drastically.

In computers, information is processed digitally using binary numbers. This means that the information is expressed by the sequence of two signals, 0 and 1. In physical terms 1 corresponds to an electric current or magnetic field ('light on'), while 0 means the absence of current or magnetic field ('light off'). ASCII[5] standardisation now prevails, whereby each

[1] It was introduced by Major Joseph Mauborgne, head of the cryptographic research division of the American army; see Singh, The Code Book (1999), 151.
[2] cf. Singh, The Code Book (1999), 151 et seq.
[3] cf. Wobst, *Abenteuer Kryptologie* [The Adventure of Cryptography], 2nd ed. (1998), p.60.
[4] Enigma was developed by Arthur Scherbius and patented in 1928. It was a little like a typewriter, as it had a keyboard on which the plain text was keyed in. By means of a peg-board and rotating drums the text was encoded in accordance with given rules and decoded at the other end on the same machine using code books.
[5] American Standard Code for Information Exchange.

letter is represented by a seven-figure combination of 0 and 1.[1] A text therefore appears as a sheet of 0s and 1s, and instead of letters it is numbers that are encrypted.

Both transposition and substitution can be used in this process. Substitution may, for example, take place by the addition of a key in the form of any row of numbers. According to the rules of binary mathematics the sum of two equal figures is zero (0+0=0 and 1+1=0) while the sum of two different figures is 1 (0+1=1). The new, encrypted row of figures arising from the addition of the key is thus a binary sequence which can either be further digitally processed or made readable again by subtracting the added key.

The use of computers made it possible to generate coded texts, using powerful encryption algorithms, which offer practically no starting-points for codebreakers. Decryption now entails trying all possible keys. The longer the key, the more likely it is that this attempt will be thwarted, even using very powerful computers, by the time it would take. There are therefore usable methods which may be regarded as secure at the present state of technology.

11.2.4. Standardisation and the deliberate restriction of security

As computers became more widely available in the 1970s, the need for the standardisation of encryption systems grow ever more urgent, since only in this way could firms communicate securely with business partners without incurring disproportionate costs. The first moves were made in the USA.

Powerful encryption systems can also be used for unlawful purposes or by potential military opponents; they may also make electronic espionage difficult or impossible. For that reason, the NSA urged that firms should be offered a sufficiently secure encryption standard, but one which the NSA itself could decrypt, by virtue of its exceptional technical capabilities. With that aim in mind, the length of the key was restricted to 56 bits. This reduces the number of possible keys to 100 000 000 000 000 000[2]. On 23 November 1976 Horst Feistel's so-called Lucifer key was officially adopted in its **56-bit version** under the name Data Encryption Standard (DES) and for the next 25 years represented the official American encryption standard[3]. This standard was also adopted in Europe and Japan, in particular in the banking sector. Media claims to the contrary, the DES algorithm has not yet been broken, but hardware now exists which is powerful enough to try all possible keys (brute force attack). In contrast, Triple DES, which has a 112-bit key, is still regarded as secure. The successor to DES, the Advanced Encryption Standard (AES), is a European process[4] which was developed under the name Rijndael in Louvain, Belgium. **It is fast and is regarded as secure, since it incorporates no key-length restriction.** The reason for this lies in a change in American policy on cryptography (see paragraph 1.4.).

Standardisation makes it much easier for firms to employ encryption. What remained, however, was the problem of key exchange.

---

[1] A= 1000001, B= 1000010, C=1000011, D=1000100, E= 1000101, etc.
[2] In binary terms, this number consists of 56 zeros and ones. See Singh, The Code Book (1999), p. 3.
[3] See Singh, The Code Book (1999), p. 302 et seq.
[4] It was created by two Belgian cryptographers working at the Catholic University of Louvain, Joan Daemen and Vincent Rijmen.

11.3. The problem of the secure distribution/handover of keys

11.3.1. Asymmetric encryption: the public-key process

As long as a system works with a key which is employed both for encryption and decryption (symmetric encryption), it is difficult to use with **large numbers** of communication partners. The key must be handed over to every new communication partner **in advance** in such a way that no third party gains access to it. This is difficult for firms in practical terms, and feasible for private individuals only in rare cases.

Asymmetric encryption offers a solution to this problem: two different keys are used for encryption and decryption. The message is encrypted using a key which may perfectly well be in the public domain, the so-called **public key**. However, the process works only in one direction, with the result that decryption is no longer possible using the public key. For that reason, anybody who wishes to receive an encrypted message may send a communication partner via an unsecured route the public key required to encrypt the message. The received message is then decrypted using a different key, the **private key**, which is kept secret and which is not forwarded to communication partners[1]. The process can best be understood on the basis of a comparison with a padlock: anyone can snap a padlock together and, by so doing, secure a trunk; the padlock can only be opened, however, by a person with the right key[2]. Although the public and private keys are linked, the private key cannot be calculated on the basis of the public key.

Ron Rivest, Adi Shamir and Leonard Adleman invented an asymmetric encryption process which has been named after them (RSA process). In a one-way (trapdoor) function the result of the multiplication of two very large prime numbers is used as a component of the public key. The text is then encrypted using that key. Decryption is dependent on knowledge of the two prime numbers employed. However, there is no known mathematical process by means of which the large integers resulting from the multiplication of two prime numbers can be factored in such a way as to determine what those prime numbers were. At present, all possible combinations must be tried systematically. Given the present state of mathematical knowledge, therefore, the process is secure, provided that sufficiently large prime numbers are chosen. The only risk is that at some stage a brilliant mathematician will discover a quicker factoring method. Thus far, however, even the best efforts have proved fruitless[3]. Many people even claim that the problem is insoluble, but this theory has not yet been proved[4].

By comparison with symmetric processes (e.g. DES), however, public-key encryption requires much more PC calculation time or the use of rapid, large-scale computers.

[1] The idea of asymmetric encryption using the public-key process was devised by Whitfield Diffie and Martin Hellmann.
[2] Singh, The Code Book (1999), p. 327.
[3] See Buchmann, Factoring large integers, Spektrum der Wissenschaft 2, 1999, pp. 6 et seq.
[4] See Singh, The Code Book (1999), pp. 335 et seq.

11.3.2. Public-key encryption for private individuals

In order to make the public-key process generally accessible, Phil Zimmermann came up with the idea of linking the public-key process, which involves a great deal of calculation, with a faster symmetric process. The message itself should be encrypted using an asymmetric process, the IDEA process developed in Zurich, but the key to the symmetric encryption would be exchanged at the same time, as in the public-key process. Zimmermann developed a user-friendly programme (Pretty Good Privacy) which created the requisite key and carried out the encryption at the push of a button (or the click of a mouse). The programme was placed on the Internet, from where anyone could download it. PGP was ultimately bought by the American firm NAI, but is still made available to private individuals free of charge[1]. The source text for the earlier versions has been published, so it can be assumed that no backdoors have been incorporated. Unfortunately, the source texts for the newest version, PGP 7, which is characterised by an exceptionally user-friendly graphic interface, are no longer published.

There is, however, a further implementation of the Open PGP Standard: GnuPG. GnuPG offers the same encryption methods as PGP, and is also compatible with PGP. However, it is freeware, its source code is known and any individual can use it and pass it on. The Federal German Ministry for Economics and Technology has promoted the porting of GnuPG on Windows and the development of a graphic interface; unfortunately, however, these functions have not yet been fully developed. According to the information available to your rapporteur, work is continuing.

There are also rival standards to OpenPGP, such as S/MIME, which are supported by many e-mail programmes. Here, your rapporteur has no information on free implementation.

11.3.3. Future processes

In the future quantum cryptography may open up new prospects for secure key exchange. It would ensure that the interception of a key exchange could not pass unnoticed. If polarised photons are transmitted, the fact of their polarisation cannot be established without altering that polarisation. Eavesdroppers on the line could thus be detected with 100% certainty. Only those keys which had not been intercepted would then be used. In experiments, transmission over 48 km via fibreoptic cable and over 500 m through the air has already been achieved[2].

11.4. Security of encryption products

In the discussion on the actual level of security of encryption processes the accusation has repeatedly been made that American products contain backdoors. For example, Excel made headlines here in Europe when it was suggested that in the European version of its programme half the key is revealed in the file header. Microsoft also gained media attention when a hacker claimed to have discovered an 'NSA key' hidden in the programme, a claim which was of course strongly denied by Microsoft. Since Microsoft has not revealed its source code, any assessment amounts to pure speculation. At all events, the earlier versions of PGP and

[1] Information on the software can be found at www.pgpi.com.
[2] On quantum cryptology, see Wobst, Abenteuer Kryptographie[2] (1998), pp. 224 et seq.

GnuPG can be said with a great degree of certainty not to contain such a backdoor, since their source text has been disclosed.

11.5. Encryption in conflict with state interests

11.5.1. Attempts to restrict encryption

Many states initially ban the use of encryption software or cryptographic equipment and make exceptions only subject to prior authorisation. The states concerned are not just dictatorships such as China, Iran or Iraq. Democratic states have also imposed legal restrictions on the use or purchase of encryption programmes or equipment. It would appear that communications are to be protected against being read by unauthorised private individuals, but that the state should retain the possibility of intercepting such communications, if necessary on the basis of specific legal provisions. The authorities' loss of technical superiority is thus made good by means of legal bans. For example, until recently France imposed a general ban on the use of cryptography, granting authorisations only in individual cases. A few years ago in Germany a debate arose concerning restrictions on encryption and the compulsory submission of a key to the authorities. In the past, the USA has taken a different course, imposing restrictions on key length.

11.5.2. The significance of secure encryption for e-commerce

By now, these attempts should have been shown, once and for all, to be futile. The state's interest in having access to encryption processes and thus to the plain texts does not only stand in opposition to the right to privacy, but also to entrenched economic interests. E-commerce and electronic banking are dependent on secure communications via the Internet. If this cannot be guaranteed, these techniques are doomed to failure, owing to a lack of customer confidence. This link explains the about-turn in American or French policy on cryptography.

It should be pointed out here that there are two reasons why e-commerce needs secure encryption processes: not only in order to encrypt messages, but also to prove beyond doubt the identity of business partners. The electronic signature procedure can be carried out using a reversal of the public-key process: the private key is used to encrypt the signature, and the public key to decrypt it. This form of encryption confirms the authenticity of the signature. Through the use of the public key, any individual can convince another of his or her genuineness, but he or she cannot imitate the signature itself. This function is also built into PGP as an additional user-friendly feature.

11.5.3. Problems for business travellers

In some states business travellers are prohibited from using encryption programmes on the laptop computers they carry with them, ruling out any protection of communications with their own firm or the data stored on those computers.

11.6. Practical issues in connection with encryption

When answering the question of what persons, and under what circumstances, should be advised to employ encryption, a distinction must be drawn between private individuals and firms.

As far as private individuals are concerned, it must be clearly stated that the encryption of fax and telephone messages using a cryptotelephone or cypherfax is not really a workable option, not only because the cost of purchasing such equipment is relatively high, but also because their use presupposes that the interlocutor also has such equipment available, which is doubtless only very rarely the case.

In contrast, e-mails can and should be encrypted by everyone. The oft-repeated claim that a person has no secrets and thus has no need to encrypt messages must be countered by pointing out that written messages are not normally sent on postcards. However, an unencrypted e-mail is nothing other than a letter without an envelope. The encryption of e-mails is secure and relatively straightforward and user-friendly systems, such as PGP/GnuPG, are already available, even free of charge, to private individuals on the Internet. Unfortunately, they are not yet sufficiently widely distributed. The public authorities should set a good example and themselves employ encryption as a standard practice in order to demystify the process.

As far as firms are concerned, they should take strict measures to ensure that sensitive information is only transmitted via secure media. This may seem obvious, and no doubt is for large undertakings, but in small- and medium-sized firms in particular internal information is often transmitted via unencrypted e-mails, because awareness of the problem is not sufficiently well developed. In this connection, it can only be hoped that industry associations and chambers of commerce will step up their efforts to increase that awareness. Admittedly, the encryption of e-mails is only one security aspect amongst many, and serves no purpose if the information is made available to others prior to encryption. The implication is that the entire working environment must be protected, thereby guaranteeing the security of a firm's premises, and checks must be carried out on persons entering offices and accessing computers. In addition, unauthorised access to information via the firm's network must be prevented by means of the introduction of corresponding firewalls. Here, particular dangers are posed by the linking of the firm's internal network and the Internet. If security is to be taken seriously, only those operating systems should be used whose source code has been published and checked, since only then can it be determined with certainty what happens to the data. Firms are thus faced with a wide variety of tasks in the security sphere. Many businesses have already been set up to provide security advice and arrangements at affordable prices, and the supply of such services is expanding steadily in line with demand. In addition, however, it must be hoped that industry associations and chambers of commerce take up this issue, particularly in order to draw the attention of small firms to the problem of security and to support efforts to devise and implement comprehensive protection arrangements.

12. The EU's external relations and intelligence gathering

12.1. Introduction

With the adoption of the Maastricht Treaty in 1991, the Common Foreign and Security Policy (CFSP) was established in its most elementary form as a new policy instrument for the European Union. Six years later the Amsterdam Treaty gave further structure to the CFSP and created the possibility for common defence initiatives within the European Union, whilst maintaining the existing alliances. On the basis of the Amsterdam Treaty and with the experiences in Kosovo in mind, the Helsinki European Council of December 1999 launched the European Security and Defence Initiative. This initiative aims at the creation of a multinational force of between 50 000 and 60 000 troops by the second half of 2003. The existence of such a multinational force will make the development of an autonomous intelligence capacity inevitable. The simple integration of the existing WEU intelligence capacity will be insufficient for this purpose. Further cooperation between the intelligence agencies of the Member States, well beyond the existing forms of cooperation, cannot be avoided.

However, the further development of the CFSP is not the only factor leading to closer cooperation among the Union's intelligence services. Further economic integration within the European Union will likewise necessitate a more intensive cooperation in the field of intelligence collection. A united European economic policy implies a united perception of economic reality in the world outside the European Union. A united position in trade negotiations within the WTO or with third countries calls for joint protection of the negotiating position. Strong European industries need joint protection against economic espionage from outside the European Union.

It must finally be emphasised that further development of the Union's second pillar and the Union's activities in the field of Justice and Home Affairs will inevitably also lead to further cooperation between intelligence services. In particular, the joint fight against terrorism, illegal trade in arms, trafficking of human beings, and money laundering cannot take place without intensive cooperation between intelligence services.

12.2. Scope for cooperation within the EU

12.2.1. Existing cooperation

Although there is a long tradition within the intelligence services of only trusting the information they collect themselves and maybe even of distrust between the different intelligence services within the European Union, cooperation between services is already gradually increasing. Frequent contacts do exist within the framework of NATO, the WEU and within the European Union. And whereas, within the framework of NATO, the intelligence services are still heavily dependent on the far more sophisticated contributions from the United States, the establishment of the WEU satellite centre in Torrejon (Spain) and the creation of an intelligence section attached to the WEU headquarters have contributed to more autonomous European action in this field.

12.2.2. Advantages of a joint European intelligence policy

In addition to these developments already taking place, it must be emphasised that there are objective advantages to a joint European intelligence policy. These advantages may be described as follows.

12.2.2.1. Professional advantages

First of all there is simply too much classified and unclassified material available to be collected, analysed, and evaluated by any single agency or under any single bilateral agreement in Western Europe. The demands on intelligence services range from defence intelligence, through intelligence on third states' internal and international economic policies, to intelligence in support of the fight against organised crime and drug trafficking. Even if cooperation existed only on the most basic level, i.e. as regards the collection of open-source intelligence (OSINT), the results of this cooperation would already be of great importance for the European Union's policies.

12.2.2.2. Budget advantages

In the recent past budgets for intelligence collection have been cut and, in some cases, are still being reduced. At the same time, the demand for information and therefore intelligence has grown. These reduced budgets do not only make this cooperation desirable but, in the long run, also profitable. In particular, in the case of establishing and maintaining technical facilities, joint operations are of interest when money is scarce but also when it comes to evaluating the collected information. Further cooperation will increase the effectiveness of intelligence collection.

12.2.2.3. Political advantages

In principle, collected intelligence is used to give governments the possibility of better and better-founded decision-making. Further political and economic integration in the European Union demands that intelligence should be available at European level and should also be based on more than one single source.

12.2.3. Concluding remarks

These objective advantages merely illustrate the growing importance of cooperation within the European Union. In the past nation states used to guarantee their own external security, internal order, national prosperity and cultural identity. Today, the European Union is in many fields in the process of taking up a role at least complementary to that of the nation state. It is inconceivable that the intelligence services will be the last and only area not affected by the process of European integration.

12.3. Cooperation beyond EU level

Following the Second World War cooperation in the field of intelligence collection did not at first take place at European level, but far more at transatlantic level. It has already been shown that very close relations in the field of intelligence gathering were established between the United Kingdom and the United States. But also in the field of defence intelligence within the

framework of NATO and beyond, the United States was and still is the absolutely dominant partner. The major question therefore is this: will growing European cooperation in the field of intelligence gathering seriously disrupt relations with the United States, or might it lead to a strengthening of those relations? How will EU/US relations develop under the new Bush Administration? And, in particular, how will the special relationship between the United States and the United Kingdom be maintained in this framework?

Some take the view that there need not be a contradiction between the British/US special relationship and the further development of the CFSP. Others believe that intelligence gathering may be precisely the issue which forces the United Kingdom to decide whether its destiny is European or transatlantic. Britain's intimate links with the US (and with the other partners in the UKUSA agreement) may make it more difficult for other EU states to share intelligence amongst themselves – because Britain may be less interested in intra-European sharing, and because its EU partners may trust Britain less. Equally, if the US believes that Britain has developed special links with its EU partners, and that this is part of a European special agreement, the US may become reluctant to continue sharing its intelligence with the United Kingdom. Closer EU cooperation in the field of intelligence may therefore constitute a serious test of the European ambitions of the United Kingdom and of the EU's capacity for integration.

In the present circumstances it is, however, highly unlikely that even extremely rapid progress in cooperation among the European partners can, in the short and even in the longer term, offset the technological advantage enjoyed by the United States. The European Union will not be able to establish a sophisticated network of SIGINT satellites, imaging satellites and ground stations. The European Union will not be able to develop, in the short term, the highly sophisticated network of computers required for the selection and evaluation of the collected material. The European Union will not be prepared to make available the budgetary resources needed to develop a true alternative to the intelligence efforts of the United States. Purely from a technological and budgetary viewpoint, therefore, it will be in the interests of the European Union to maintain a close relationship with the United States in the field of intelligence collection. But also from a more political point of view, it will be important to maintain and, where necessary, strengthen relationships with the United States, in particular in the context of the joint fight against organised crime, terrorism, drugs and arms trafficking and money laundering. Joint intelligence operations are necessary to support a joint fight. Joint peacekeeping actions, such as in former Yugoslavia, demand a greater European contribution in all areas.

On the other hand, growing European awareness should be accompanied by greater European responsibility. The European Union should become a more equal partner, not only in the economic field, but also in the field of defence and therefore in the field of intelligence collection. A more autonomous European intelligence capacity should therefore not be seen as weakening transatlantic relations, but should be used to strengthen them by establishing the European Union as a more equal and more capable partner. At the same time, the European Union must make independent efforts to protect its economy and its industry against illegal and unwanted threats such as economic espionage, cyber-crime, and terrorist attacks. However, transatlantic understanding is necessary in the field of industrial espionage. The European Union and the United States should agree on a set of rules laying down what is and what is not allowed in this area. With a view to strengthening transatlantic cooperation in this

field, a joint initiative could be undertaken at WTO level using that organisation's mechanisms to safeguard fair economic development worldwide.

12.4. Final remarks

Although the issue of the protection of European citizens' privacy must remain fundamental, the further development of a joint European Union intelligence capacity should be considered necessary and inevitable. Cooperation with third countries, and in particular the United States, should be maintained and, very possibly, strengthened. This does not necessarily mean that European SIGINT activities should automatically be integrated in an independent European Union ECHELON system, or that the European Union should become a full partner in the present UKUSA Agreement. However, the development of proper European responsibility in the field of intelligence collection must be actively considered. An integrated European intelligence capacity demands, at the same time, a system of European political control over the activities of these agencies. Decisions will have to be taken on the procedure for assessing intelligence and for taking the political decisions which result from an analysis of intelligence reports. The lack of such a system of political control, and therefore of political awareness and responsibility for the process of intelligence collection, would be detrimental to the process of European integration.

13. Conclusions and recommendations

13.1. Prefatory remark

This chapter summarises the committee's findings and possible conclusions. It has no pretensions to being definitive. The rapporteur's aim is rather to provide a basis for the political debate which is now to be conducted within the committee. The text will subsequently need to be amended so as to incorporate the fruits of that debate.

13.2. Conclusions

The existence of a global system for intercepting private and commercial communications (the ECHELON interception system)

That a global system for intercepting communications exists, operating by means of cooperation proportionate to their capabilities among the USA, the UK, Canada, Australia and New Zealand under the UKUSA Agreement, is no longer in doubt. That its name is in fact ECHELON seems likely in view of the evidence, but this is a relatively minor detail. What is important is that its purpose is to intercept private and commercial communications, and not military communications.

Analysis has revealed that the system cannot be nearly as extensive as some sections of the media have assumed.

The limits of the interception system

The surveillance system depends upon worldwide interception of satellite communications. However, in areas characterised by a high volume of communications only a very small proportion of those communications are transmitted by satellite. This means that the majority of communications cannot be intercepted by earth stations, but only by tapping cables and intercepting radio signals. However, inquiries have shown that the ECHELON states have access to only a very limited proportion of cable and radio communications, and, owing to the large numbers of personnel required, can analyse only a limited proportion of those communications.

The possible existence of other interception systems

Since intercepting communications is a method of spying commonly employed by intelligence services, other states might also operate similar systems, provided that they have the required funds and the right locations. Geographically at least – thanks to its overseas territories – France is the only EU Member State which could set up a global interception system by itself. There is evidence that Russia might also be able to operate such a system.

Compatibility with EU law

As regards the question of the compatibility of a system of the ECHELON type with EU law, it is necessary to distinguish between two scenarios. If a system is used purely for intelligence

purposes, there is no violation of EU law, since operations in the interests of state security are not subject to the EC Treaty, but would fall under Title V of the Treaty on European Union (CFSP), although at present that title lays down no provisions on the subject, so no criteria are available. If, on the other hand, the system is abused for the purposes of gathering competitive intelligence, such action is at odds with the Member States' duty of loyalty and with the concept of a common market based on free competition. If a Member State participates in such a system, it violates EC law.

Compatibility with the fundamental right to respect for private life (Article 8 of the ECHR)

Any interception of communications represents serious interference with an individual's exercise of the right to privacy. Article 8 of the ECHR, which guarantees respect for private life, permits interference with the exercise of that right only in the interests of national security, in so far as this is in accordance with domestic law and the provisions in question are generally accessible and lay down under what circumstances, and subject to what conditions, the state may undertake such interference. Interference must be proportionate: thus competing interests need to be weighed up and it is not enough that the interference should merely be useful or desirable.

An intelligence system which intercepted all communications without any guarantee of compliance with the principle of proportionality would not be compatible with the ECHR. It would also constitute a violation of the ECHR if the rules governing the surveillance of communications lacked a legal basis, if the rules were not generally accessible or if they were so formulated that their implications for the individual were unforeseeable. Since most of the rules governing the activities of US intelligence services abroad are classified, compliance with the principle of proportionality is at least doubtful and breaches of the principles of accessibility and foreseeability laid down by the European Court of Human Rights probably occur. Although the USA is not itself an ECHR contracting party, the Member States must nevertheless act in a manner consistent with the ECHR. The Member States cannot circumvent the requirements imposed on them by the ECHR by allowing other countries' intelligence services, which are subject to less stringent legal provisions, to work on their territory, since otherwise the principle of legality, with its twin components of accessibility and forseeability, would become a dead letter and the case law of the European Court of Human Rights would be deprived of its substance.

In addition, the lawful operations of intelligence services are consistent with fundamental rights only if adequate arrangements exist for monitoring them, in order to counterbalance the risks inherent in secret activities performed by a part of the administrative apparatus. As the European Court of Human Rights has expressly stressed the importance of an efficient system for monitoring intelligence operations, there are grounds for concern in the fact that some Member States do not have parliamentary monitoring bodies of their own responsible for scrutinising the secret services.

Are EU citizens adequately protected against intelligence services?

As the protection enjoyed by EU citizens depends on the legal situation in the individual Member States, which varies very substantially, and since in some cases parliamentary monitoring bodies do not even exist, the degree of protection can hardly be said to be

adequate. It is in the fundamental interests of European citizens that their national parliaments should have a specific, formally structured monitoring committee responsible for supervising and scrutinising the activities of the intelligence services. But even where monitoring bodies do exist, there is a strong temptation for them to concentrate more on the activities of domestic intelligence services, rather than those of foreign intelligence services, since as a rule it is only the former which affect their own citizens.

In the event of cooperation between intelligence services under the CFSP, the institutions must introduce adequate measures to protect European citizens.

Industrial espionage

Part of the remit of foreign intelligence services is to gather economic data, such as details of developments in individual sectors of the economy, trends on commodity markets, compliance with economic embargoes, observance of rules on supplying dual-use goods, etc. For these reasons, the firms concerned are often subject to surveillance. The situation becomes intolerable when intelligence services allow themselves to be used for purposes of gathering competitive intelligence by spying on foreign firms with the aim of securing a competitive advantage for firms in the home country. It is frequently maintained that ECHELON has been used in this way, but no such case has been substantiated.

The fact is that sensitive commercial data are mostly kept inside individual firms, so that competitive intelligence-gathering primarily involves efforts to obtain information through members of staff or through people planted in the firm for this purpose or else by hacking into internal computer networks. Only if sensitive data are transmitted externally by cable or radio (satellite) can a communications surveillance system be used for competitive intelligence-gathering. This applies systematically in the following three cases:
- in the case of firms which operate in three time zones, so that interim results are sent from Europe to America and on to Asia;
- in the case of videoconferencing within multinationals using VSAT or cable;
- if vital contracts are being negotiated on the spot (e.g. for the building of plants, telecommunications infrastructure, the creation of new transport systems, etc.) and it is necessary to consult the company's head office.

Possible self-protection measures

Firms must secure the whole working environment and protect all communications channels which are used to send sensitive information. Sufficiently secure encryption systems exist at affordable prices on the European market. Private individuals should also be urged to encrypt e-mails: an unencrypted e-mail message is like a letter without an envelope. Relatively user-friendly systems exist on the Internet which are even made available for private use free of charge.

Cooperation among intelligence services within the EU

The EU has reached agreement on the coordination of intelligence-gathering by intelligence services as part of the development of its own security and defence policy, although ccooperation with other partners in these areas will continue. Cooperation among intelligence

services within the EU seems desirable on the grounds that, firstly, a common security policy which did not involve the secret services would not make sense and, secondly, it would have numerous professional, financial and political advantages. It would also accord better with the idea of the EU as a partner on an equal footing with the United States and could bring together all the Member States in a system which complied fully with the ECHR. The European Parliament would of course have to exercise appropriate monitoring.

13.3. Recommendations

Conclusion and amendment of international agreements on the protection of citizens and firms

1. The Secretary-General of the Council of Europe is called upon to submit to the Ministerial Committee an analysis of whether the protection of private life guaranteed in Article 8 of the ECHR should be brought into line with modern communication and interception methods by means of an additional protocol or, together with the provisions governing data protection, as part of a revision of the Convention on Data Protection, with the proviso that this should neither undermine the level of legal protection established by the European Court of Human Rights nor reduce the flexibility which is vital if future developments are to be taken into account.

2. The Member States are called upon to establish a European platform in order to review the legal provisions guaranteeing postal and communications secrecy and, in addition, to reach agreement on a joint text which affords all European citizens, throughout the territory of the Member States, protection of privacy as defined in Article 7 of the Charter of Fundamental Rights of the European Union and which, moreover, guarantees that the activities of intelligence services are carried out in a manner consistent with fundamental rights, in keeping with the conditions set out in Chapter 8 of this report, and in particular Section 8.3.4., as derived from Article 8 of the ECHR.

3. The member countries of the Council of Europe are called upon to adopt an additional protocol which enables the European Communities to accede to the ECHR or to consider other measures designed to prevent disputes relating to case law arising between the European Court of Human Rights and the Court of Justice of the European Communities.

4. The UN Secretary-General is called upon to instruct the competent committee to put forward proposals designed to bring Article 17 of the International Covenant on Civil and Political Rights, which guarantees the protection of privacy, into line with technical innovations.

5. The USA is called upon to sign the Additional Protocol to the International Covenant on Civil and Political Rights, so that complaints by individuals concerning breaches of the Covenant by the USA can be submitted to the Human Rights Committee set up under the Covenant; calls on the relevant American NGOs, in particular the ACLU (American Civil Liberties Union) and the EPIC (Electronic Privacy Information Center), to exert pressure on the US Administration to that end.

National legislative measures to protect citizens and firms

6. The Member States are called upon to review their own legislation on the operations of the intelligence services to ensure that it is consistent with fundamental rights.

7. The Member States are called upon to aspire to a common level of protection against intelligence operations based on the highest level of protection which exists in any Member State, since as a rule it is citizens of other states, and hence also of other Member States, that are affected by the operations of foreign intelligence services.

8. The EU institutions are called upon, in the event of cooperation between intelligence services under the CFSP, to introduce adequate measures to protect European citizens; the European Parliament, as the logical monitoring body, must for its part create the preconditions for the supervision of this highly sensitive area in order to make it realistic – and indeed defensible – to insist on being granted the necessary monitoring rights.

Specific legal measures to combat industrial espionage

9. The Member States are called upon to consider to what extent industrial espionage and the payment of bribes as a means of securing contracts can be combated by means of European and international legal provisions and, in particular, whether WTO rules could be adopted which take account of the distortions of competition brought about by such practices, for example by rendering contracts obtained in this way null and void.

10. The Member States are called upon to undertake by means of a clear joint declaration not to engage in industrial espionage against one another, thereby signifying their compliance with the letter and spirit of the EC Treaty;

Measures concerning the implementation of the law and the monitoring of that implementation

11. The national parliaments which have no parliamentary monitoring body responsible for scrutinising the activities of the intelligence services are called upon to set up such a body;

12. The monitoring bodies responsible for scrutinising the activities of the secret services are called upon, when exercising their monitoring powers, to attach great importance to the protection of privacy, regardless of whether the individuals concerned are their own nationals, other EU nationals or third-country nationals.

13. The Member States' intelligence services are called upon to accept data from other intelligence services only in cases where such data has been obtained in accordance with the conditions laid down by their own domestic law, as Member States cannot evade the obligations arising from the ECHR by using other intelligence services.

14. Germany and England are called upon to make the authorisation of further communications interception operations by US intelligence services on their territory conditional on their compliance with the ECHR, i.e. to stipulate that they should be

consistent with the principle of proportionality, that their legal basis should be accessible and that the implications for individuals should be foreseeable, and to introduce corresponding, effective monitoring measures, since they are responsible for ensuring that intelligence operations authorised or even merely tolerated on their territory respect human rights.

Measures to encourage self-protection by citizens and firms

15. The Commission and Member States are called upon to develop programmes to foster awareness of security problems among citizens and firms and at the same time to provide practical assistance in designing and implementing comprehensive protection strategies.

16. The Commission and Member States are urged to devise appropriate measures to promote, develop and manufacture European encryption technology and software and above all to support projects aimed at developing user-friendly open-source encryption software.

17. The Commission and Member States are called upon to promote software projects whose source text is made public (open-source software), as this is the only way of guaranteeing that no backdoors are built into programmes.

18. The European institutions and the public administrations of the Member States are called upon systematically to encrypt e-mails, so that ultimately encryption becomes the norm.

Other measures

19. Firms are called upon to cooperate more closely with counter-espionage services, and particularly to inform them of attacks from outside for the purposes of industrial espionage, in order to improve the services' efficiency.

20. The Commission is called upon to put forward a proposal to set up a European advisory centre to deal with issues relating to the security of the information held by firms, with the twin task of increasing awareness of the problem and providing practical assistance.

21. The European Parliament is called upon to hold an international congress on the protection of privacy against telecommunications surveillance in order to provide NGOs from Europe, the USA and other countries with a forum for discussion of the cross-border and international aspects of the problem and coordination of areas of activity and action.