EUROPEAN PARLIAMENT

1999 *2004*

Session document

FINAL
A5-0264/2001
PAR1

11 July 2001

REPORT

on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))

Part 1: Motion for a resolution
Explanatory statement

Temporary Committee on the ECHELON Interception System

Rapporteur: Gerhard Schmid

'Sed quis custodiet ipsos custodes.'
Juvenal (ca. 60 to 130 AD), Sat. 6, 347

CONTENTS

Page

PROCEDURAL PAGE 9

MOTION FOR A RESOLUTION 10

EXPLANATORY STATEMENT 21

1. **Introduction:** **21**

1.1. The reasons for setting up the committee 21
1.2. The claims made in the two STOA studies on a global interception system codenamed ECHELON 21
1.2.1. The first STOA report of 1997 21
1.2.2. The 1999 STOA reports 21
1.3. The mandate of the committee 22
1.4. Why not a committee of inquiry? 22
1.5. Working method and schedule 23
1.6. Characteristics ascribed to the ECHELON system 23

2. The operations of foreign intelligence services **25**

2.1. Introduction 25
2.2. What is espionage? 25
2.3. Espionage targets 25
2.4. Espionage methods 25
2.4.1. Human intelligence 26
2.4.2. Processing of electromagnetic signals 26
2.5. The operations of certain intelligence services 27

3. Technical conditions governing the interception of telecommunications **30**

3.1. The interceptibility of various communication media 30
3.2. The scope for interception on the spot 30
3.3. The scope for a worldwide interception system 31
3.3.1. Access to communication media 31
3.3.2. Scope for the automatic analysis of intercepted communications: the use of filters 35
3.3.3. The example of the German Federal Intelligence Service 35

4. Satellite communications technology 37

4.1. The significance of telecommunications satellites 37
4.2. How a satellite link operates 38
4.2.1. Geostationary satellites 38
4.2.2. The route followed by signals sent via a satellite communication link 38
4.2.3. The most important satellite communication systems 39
4.2.4. The allocation of frequencies 43
4.2.5. Satellite footprints 43
4.2.6. The size of antennae required by an earth station 44
4.3. Satellite communications for military purposes 45
4.3.1. General 45
4.3.2. Frequencies used for military purposes 45
4.3.3. Size of the receiving stations 45
4.3.4. Examples of military communications satellites 45

5. Clues to the existence of at least one global interception system 47

5.1. Why is it necessary to work on the basis of clues? 47
5.1.1. Evidence of interception activity on the part of foreign intelligence services 47
5.1.2. Evidence for the existence of stations in the necessary geographical areas 47
5.1.3. Evidence of a close intelligence association 48
5.2. How can a satellite communications interception station be recognised? 48
5.2.1. Criterion 1: accessibility of the installation 48
5.2.2. Criterion 2: type of antenna 48
5.2.3. Criterion 3: size of antenna 49
5.2.4. Criterion 4: evidence from official sources 49
5.3. Publicly accessible data about known interception stations 50
5.3.1. Method 50
5.3.2. Detailed analysis 50
5.3.3. Summary of the findings 59
5.4. The UKUSA Agreement 59
5.4.1. The historical development of the UKUSA Agreement 59
5.4.2. Evidence for the existence of the agreement 61
5.5. Evaluation of declassified American documents 62
5.5.1. Nature of documents 62
5.5.2. Content of documents 63
5.5.3. Summary 66
5.6. Information from authors and journalists specialised in this field 67
5.6.1. Nicky Hager's book 67
5.6.2. Duncan Campbell 68
5.6.3. Jeff Richelson 69
5.6.4. James Bamford 69
5.6.5. Bo Elkjaer and Kenan Seeberg 70
5.7. Statements by former intelligence service employees 71
5.7.1. Margaret Newsham (former NSA employee) 71
5.7.2. Wayne Madsen (former NSA employee) 71
5.7.3. Mike Frost (former Canadian secret service employee) 71

5.7.4. Fred Stock (former Canadian secret service employee) 72
5.8. Information from government sources 72
5.8.1. USA 72
5.8.2. UK 72
5.8.3. Australia 73
5.8.4. New Zealand 73
5.8.5. The Netherlands 73
5.8.6. Italy 74
5.9. Questions to the Council and Commission 74
5.10. Parliamentary reports 75
5.10.1. Reports by the Comité Permanent R, Belgium's monitoring committee 75
5.10.2. Report by the French National Assembly's Committee on National Defence 75
5.10.3. Report of the Italian Parliament's Committee on Intelligence and Security Services and State Security 76

6. Might there be other global interception systems? 77

6.1. Requirements of such a system 77
6.1.1. Technical and geographical requirements 77
6.1.2. Political and economic requirements 77
6.2. France 77
6.3. Russia 78
6.4. The other G-8 States and China 79

7. Compatibility of an 'ECHELON' type communications interception system with Union law 80

7.1. Preliminary considerations 80
7.2. Compatibility of an intelligence system with Union law 80
7.2.1. Compatibility with EC law 80
7.2.2. Compatibility with other EU law 81
7.3. The question of compatibility in the event of misuse of the system for industrial espionage 82
7.4. Conclusion 82

8. The compatibility of communications surveillance by intelligence services with the fundamental right to privacy 83

8.1. Communications surveillance as a violation of the fundamental right to privacy 83
8.2. The protection of privacy under international agreements 83
8.3. The rules laid down in the ECHR 84
8.3.1. The importance of the ECHR in the EU 84
8.3.2. The geographical and personal scope of the protection provided under the ECHR 85
8.3.3. The admissibility of telecommunications surveillance pursuant to Article 8 of the ECHR 85
8.3.4. The significance of Article 8 of the ECHR for the activities of intelligence services) 86

8.4. The requirement to monitor closely the activities of other countries' intelligence services 87
8.4.1. Inadmissibility of moves to circumvent Article 8 of the ECHR through the use of other countries' intelligence services 87
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 88

9. Are EU citizens adequately protected against the activities of intelligence services? 91

9.1. Protection against the activities of intelligence services: a task for the national parliaments 91
9.2. The powers enjoyed by national authorities to carry out surveillance measures 91
9.3. Monitoring of intelligence services 92
9.4. Assessment of the situation for European citizens 95

10. Protection against industrial espionage 97

10.1. Firms as espionage targets 97
10.1.1. Espionage targets in detail 97
10.1.2. Competitive intelligence 98
10.2. Damage caused by industrial espionage 98
10.3. Who carries out espionage? 99
10.3.1. Company employees (insider crime) 99
10.3.2. Private espionage firms 100
10.3.3. Hackers 100
10.3.4. Intelligence services 100
10.4. How is espionage carried out? 100
10.5. Industrial espionage by states 101
10.5.1. Strategic industrial espionage by the intelligence services 101
10.5.2. Intelligence services as agents of competitive intelligence 101
10.6. Is ECHELON suitable for industrial espionage? 102
10.7. Published cases 102
10.8. Protection against industrial espionage 107
10.8.1. Legal protection 107
10.8.2. Other obstacles to industrial espionage 107
10.9. The USA and industrial espionage 108
10.9.1. The challenge for the US Administration: industrial espionage against US firms ..109
10.9.2. The attitude of the US Administration towards active industrial espionage 110
10.9.3. Legal situation with regard to the payment of bribes to public officials 111
10.9.4. The role of the Advocacy Center in promoting US exports 112
10.10. Security of computer networks 114
10.10.1. The importance of this chapter 114
10.10.2. The risks inherent in the use by firms of modern information technology 114
10.10.3. Frequency of attacks on networks 116
10.10.4. Perpetrators and methods 116
10.10.5. Attacks from outside by hackers 117

10.11. Under-estimation of the risks 117
10.11.1. Risk-awareness in firms 117
10.11.2. Risk-awareness among scientists 118
10.11.3. Risk-awareness in the European institutions 118

11. Cryptography as a means of self-protection 120

11.1. Purpose and method of encryption 120
11.1.1. Purpose of encryption 120
11.1.2. How encryption works 120
11.2. Security of encryption systems 121
11.2.1. Meaning of 'security' in encryption: general observations 121
11.2.2. Absolute security: the one-time pad 122
11.2.3. Relative security at the present state of technology 122
11.2.4. Standardisation and the deliberate restriction of security 123
11.3. The problem of the secure distribution/handover of keys 124
11.3.1. Asymmetric encryption: the public-key process 124
11.3.2. Public-key encryption for private individuals 125
11.3.3. Future processes 125
11.4. Security of encryption products 125
11.5. Encryption in conflict with state interests 126
11.5.1. Attempts to restrict encryption 126
11.5.2. The significance of secure encryption for e-commerce 126
11.5.3. Problems for business travellers 126
11.6. Practical issues in connection with encryption 127

12. The EU's external relations and intelligence gathering 128

12.1. Introduction 128
12.2. Scope for cooperation within the EU 128
12.2.1. Existing cooperation 128
12.2.2. Advantages of a joint European intelligence policy 129
12.2.3. Concluding remarks 129
12.3. Cooperation beyond EU level 129
12.4. Final remarks 131

13. Conclusions and recommendations 132

13.1. Conclusions 132
13.2. Recommendations 135

PROCEDURAL PAGE

At the sitting of 5 July 2000 the European Parliament decided, pursuant to Rule 150(2) of its Rules of Procedure, to set up a Temporary Committee on the ECHELON Interception System and laid down its mandate as outlined in Chapter 1, 1.3. With a view to fulfilling that mandate, at its constituent meeting of 9 July 2000 the Temporary Committee appointed Gerhard Schmid rapporteur.

At its meetings of 29 May, 20 June and 3 July 2001 the committee considered the draft report.

At the last meeting the committee adopted the motion for a resolution by 27 votes to 5, with 2 abstentions.

The following were present for the vote: Carlos Coelho, chairman; Elly Plooij-van Gorsel, Neil MacCormick and Giuseppe Di Lello Finuoli, vice-chairmen; Gerhard Schmid, rapporteur; Mary Elizabeth Banotti, Bastiaan Belder, Maria Berger, Charlotte Cederschiöld, Gérard M.J. Deprez, Giorgos Dimitrakopoulos, Robert J.E. Evans, Colette Flesch, Pernille Frahm, Anna Karamanou, Eva Klamt, Alain Krivine, Torben Lund, Erika Mann, Jean-Charles Marchiani, Hugues Martin, Patricia McKenna, William Francis Newton Dunn (for Jorge Salvador Hernández Mollar), Reino Paasilinna, Bernd Posselt (for Hubert Pirker), Jacques Santer (for Catherine Lalumière), Ilka Schröder, Gary Titley (for Ozan Ceyhun), Maurizio Turco, Gianni Vattimo, W.G. van Velzen, Christian Ulrik von Boetticher, Jan Marinus Wiersma and Christos Zacharakis (for Enrico Ferri).

The minority opinions and the annexes will be published separately (A5-0264/2001-Par2).

The report was tabled on 11 July 2001.

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) (2001/2098 (INI))

The European Parliament,

– having regard to its decision of 5 July 2000 to set up a Temporary Committee on the ECHELON Interception System and the mandate issued to the Temporary Committee[1],

– 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 Articles 11 and 12 of the Treaty on European Union, which impose on the Member States a binding requirement to enhance and develop their mutual political solidarity,

– 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 Article 12 of the Universal Declaration of Human Rights,

– 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, and Article 8 of which protects personal data,

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

– having regard to the work carried out by the Temporary Committee on the ECHELON Interception System, which held a large number of hearings and meetings with experts of all kinds, and in particular with senior representatives of the public and private sectors in the sphere of telecommunications and data protection, with employees of intelligence and information services, with journalists, with lawyers with expert knowledge of this area, with members of the national parliaments of the Member States, etc.,

– having regard to Rule 150(2) of its Rules of Procedure,

– having regard to the report of the Temporary Committee on the ECHELON Interception System (A5-0264/2001),

[1] OJ C 121, 24.4.2001, p. 36

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 and the consistent pattern of statements from a very wide range of individuals and organisations, including American sources, that its name is in fact ECHELON, although this is a relatively minor detail,

B. whereas there can now be no doubt that the purpose of the system is to intercept, at the very least, private and commercial communications, and not military communications, although the analysis carried out in the report has revealed that the technical capabilities of the system are probably not nearly as extensive as some sections of the media had assumed,

C. whereas, therefore, it is surprising, not to say worrying, that many senior Community figures, including European Commissioners, who gave evidence to the Temporary Committee claimed to be unaware of this phenomenon,

The limits of the interception system

D. whereas the surveillance system depends, in particular, 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 UKUSA states have access to only a very limited proportion of cable and radio communications and can analyse an even more limited proportion of those communications, and whereas, further, however extensive the resources and capabilities for the interception of communications may be, the extremely high volume of traffic makes exhaustive, detailed monitoring of all communications impossible in practice,

The possible existence of other interception systems

E. 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 France is the only EU Member State which is – thanks to its overseas territories – geographically and technically capable of operating autonomously a global interception system and also possesses the technical and organisational infrastructure to do so; whereas there is also ample evidence that Russia is likely to operate such a system,

Compatibility with EU law

F. 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 misused 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,

G. having regard to the statements made by the Council at the plenary sitting of 30 March 2000 to the effect that 'the Council cannot agree to the creation or existence of a telecommunications interception system which does not comply with the rules laid down in the law of the Member States and which breaches the fundamental principles designed to safeguard human dignity',

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

H. 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,

I. whereas an intelligence system which intercepted communications permanently and at random would be in violation of the principle of proportionality and 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, or if the interference was not proportionate; 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 foreseeability laid down by the European Court of Human Rights probably occur,

J. 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 foreseeability, would become a dead letter and the case law of the European Court of Human Rights would be deprived of its substance,

K. 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?

L. 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; whereas it would be an encouragement for proportionate interference practices, if intelligence services were obliged to notify a citizen whose communications have been intercepted of this fact afterwards, for instance five years after the interception took place,

M. whereas, in view of their size, satellite receiving stations cannot be built on the territory of a state without its consent,

N. whereas, in the event of cooperation between intelligence services under the CFSP or in the areas of justice and home affairs, the institutions must introduce adequate measures to protect European citizens,

Industrial espionage

O. 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,

P. whereas the US intelligence services do not merely investigate general economic facts but also intercept detailed communications between firms, particularly where contracts are being awarded, and they justify this on the grounds of combating attempted bribery; whereas detailed interception poses the risk that information may be used for the purpose of competitive intelligence-gathering rather than combating corruption, even though the US and the United Kingdom state that they do not do so; whereas, however, the role of the Advocacy Center of the US Department of Commerce is still not totally clear and talks arranged with the Center with a view to clarifying the matter were cancelled,

Q. whereas an agreement on combating the bribery of officials, under which bribery is criminalised at international level, was adopted by the OECD in 1997, and this provides a further reason why individual cases of bribery cannot justify the interception of communications,

R. whereas the situation becomes intolerable when intelligence services allow themselves to be used for the 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,

S. whereas, during the visit by the delegation from the Temporary Committee to the US, authoritative sources confirmed the US Congress Brown Report, indicating that 5% of intelligence gathered via non-open sources is used as economic intelligence; whereas it was estimated by the same sources that this intelligence surveillance could enable US industry to earn up to US$ 7 billion in contracts,

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

U. whereas risk and security awareness in small and medium-sized firms is often inadequate and the dangers of economic espionage and the interception of communications are not recognised,

V. whereas security awareness is not always well developed in the European institutions (with the exception of the European Central Bank, the Council Directorate-General for External Relations and the Commission Directorate-General for External Relations) and action is therefore necessary,

Possible self-protection measures

W. 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

X. 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,

Y. whereas in December 1999 in Helsinki the European Council decided to develop more effective European military capabilities with a view to undertaking the full range of Petersberg tasks in support of the CFSP; whereas the European Council decided furthermore that, in order to achieve this goal, by the year 2003 the Union should be able to deploy rapidly units of about 50 000 – 60 000 troops which should be self-sustaining, including the necessary command, control and intelligence capabilities; whereas the first steps towards such an autonomous intelligence capability have already been taken in the framework of the WEU and the standing Political and Security Committee,

Z. whereas cooperation among intelligence services within the EU seems essential 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,

AA. whereas the European Parliament is in the process of implementing the regulation on public access to European Parliament, Council and Commission documents by amending the provisions of its Rules of Procedure as regards access to sensitive documents,

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

1. States, on the basis of the information obtained by the Temporary Committee, that the existence of a global system for intercepting communications, operating with the participation of the United States, the United Kingdom, Canada, Australia and New Zealand under the UKUSA Agreement, is no longer in doubt;

2. Calls on the Secretary-General of the Council of Europe to submit to the Ministerial Committee a proposal to protect private life, as guaranteed in Article 8 of the ECHR, 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;

3. Calls on the Member States – whose laws governing the interception capabilities of the secret services contain provisions on the protection of privacy which are discriminatory – to provide all European citizens with the same legal guarantees concerning the protection of privacy and the confidentiality of correspondence;

4. Calls on the Member States of the European Union to establish a European platform consisting of representatives of the national bodies that are responsible for monitoring Member States' performance in complying with fundamental and citizens' rights in order to scrutinise the consistency of national laws on the intelligence services with the ECHR and the EU Charter of Fundamental Rights, to review the legal provisions guaranteeing postal and communications secrecy, and, in addition, to reach agreement on a recommendation to the Member States on a Code of Conduct to be drawn up which guarantees 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;

5. Calls on the Member States to adopt the EU Charter of Fundamental Rights as a legally binding and enforceable act at the next Intergovernmental Conference in order to raise the standard of protection for fundamental rights, particularly with regard to the protection of privacy;

6. 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;

7. Urges the EU institutions in the meantime to apply the fundamental rights enshrined in the Charter within the scope of their respective powers and activities;

8. 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;

9. Regards it as essential that an agreement should be negotiated and signed between the European Union and the United States stipulating that each of the two parties should observe, vis-à-vis the other, the provisions governing the protection of the privacy of citizens and the confidentiality of business communications applicable to its own citizens and firms;

10. 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

11. Urges the Member States to review and if necessary to adapt their own legislation on the operations of the intelligence services to ensure that it is consistent with fundamental rights as laid down in the ECHR and with the case law of the European Court of Human Rights;

12. Calls on the Member States to endow themselves with binding instruments which afford natural and legal persons effective protection against all forms of illegal interception of their communications;

13. Calls on the Member States to aspire to a common level of protection against intelligence operations and, to that end, to draw up a Code of Conduct (as referred to in paragraph 4) 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;

14. Calls on the Member States to negotiate with the USA a Code of Conduct similar to that of the EU;

15. Calls on those Member States which have not yet done so to guarantee appropriate parliamentary and legal supervision of their secret services;

16. Urges the Council and the Member States to establish as a matter of priority a system for the democratic monitoring and control of the autonomous European intelligence capability and other joint and coordinated intelligence activities at European level; proposes that the European Parliament should play an important role in this monitoring and control system;

17. Calls on the Member States to pool their communications interception resources with a view to enhancing the effectiveness of the CFSP in the areas of intelligence-gathering and the fight against terrorism, nuclear proliferation or international drug trafficking, in accordance with the provisions governing the protection of citizens' privacy and the confidentiality of business communications, and subject to monitoring by the European Parliament, the Council and the Commission;

18. Calls on the Member States to conclude an agreement with third countries aimed at providing increased protection of privacy for EU citizens, under which all contracting states give a commitment, where one contracting state intercepts communications in another contracting state, to inform the latter of the planned actions;

Specific legal measures to combat industrial espionage

19. Calls on the Member States to consider to what extent industrial espionage and the payment of bribes as a way 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; calls on the United States, Australia, New Zealand and Canada to join this initiative;

20. Calls on the Member States to undertake to incorporate in the EC Treaty a clause prohibiting industrial espionage and not to engage in industrial espionage against one another, either directly or with the assistance of a foreign power which might carry out operations on their territory, nor to allow a foreign power to conduct espionage operations from the soil of an EU Member State, thereby complying with the letter and spirit of the EC Treaty;

21. Calls on the Member States to undertake by means of a clear and binding instrument not to engage in industrial espionage, thereby signifying their compliance with the letter and spirit of the EC Treaty; calls on the Member States to transpose this binding principle into their national legislation on intelligence services;

22. Calls on the Member States and the US Administration to start an open US-EU dialogue on economic intelligence-gathering;

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

23. 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;

24. 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;

25. Calls on the Member States to make sure that their intelligence systems are not misused for the purposes of gathering competitive intelligence, an act at odds with the Member States' duty of loyalty and with concept of a common market based on free competition;

26. Calls on Germany and the United Kingdom 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

27. Calls on the Commission and the Member States to inform their citizens and firms about the possibility that their international communications may, under certain circumstances, be intercepted; insists that this information should be accompanied by practical assistance in designing and implementing comprehensive protection measures, including the security of information technology;

28. Calls on the Commission, the Council and the Member States to develop and implement an effective and active policy for security in the information society; insists that as part of this policy specific attention should be given to increasing the awareness of all users of modern communication systems of the need to protect confidential information; furthermore, insists on the establishment of a Europe-wide, coordinated network of agencies capable of providing practical assistance in designing and implementing comprehensive protection strategies;

29. 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;

30. 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;

31. Calls on the Commission to lay down a standard for the level of security of e-mail software packages, placing those packages whose source code has not been made public in the 'least reliable' category;

32. 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;

33. Calls on the Community institutions and the public administrations of the Member States to provide training for their staff and make their staff familiar with new encryption technologies and techniques by means of the necessary practical training and courses;

34. Calls for particular attention to be paid to the position of the applicant countries; urges that they should be given support, if their lack of technological independence prevents them from implementing the requisite protective measures;

Other measures

35. 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;

36. Instructs the Commission to have a security analysis carried out which will show what needs to be protected, and to have a protection strategy drawn up;

37. Calls on the Commission to update its encryption system in line with the latest developments, given that modernisation is urgently needed, and calls on the budgetary authorities (the Council together with Parliament) to provide the necessary funding;

38. Requests the competent committee to draw up an own-initiative report on security and the protection of secrecy in the European institutions;

39. Calls on the Commission to ensure that data is protected in its own data-processing systems and to step up the protection of secrecy in relation to documents not accessible to the public;

40. Calls on the Commission and the Member States to invest in new technologies in the field of decryption and encryption techniques as part of the Sixth Research Framework Programme;

41. Urges states which have been placed at a disadvantage by distortions of competition resulting from state aid or the economic misuse of espionage to inform the authorities and monitoring bodies of the state from which the activities were undertaken in order to put a stop to the distorting activities;

42. Calls on the Commission to put forward a proposal to establish, in close cooperation with industry and the Member States, a Europe-wide, coordinated network of advisory centres - in particular in those Member States where such centres do not yet exist - 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;

43. 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;

44. Instructs its President to forward this resolution to the Council, the Commission, the Secretary-General and Parliamentary Assembly of the Council of Europe and the governments and parliaments of the Member States and applicant countries, the United States, Australia, New Zealand and Canada.

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[2] concerning the so-called ECHELON system[3], 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 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].

---

[2] STOA (Scientific and Technological Options Assessment) is a department of the Directorate-General for Research of the European Parliament which commissions research at the request of committees. However, the documents it produces are not subject to scientific review.

[3] *Duncan Campbell*, 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, Part 2/5, in: STOA (Ed.), Development of Surveillance Technology and Risk of Abuse of Economic Information (October 1999), PE 168.184.

[4] *Steve Wright,* An appraisal of technologies of political control, STOA interim study, PE 166.499/INT.ST. (1998), 20

[5] *Duncan Campbell*, 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, Part 2/5, in: STOA (Ed.), Development of Surveillance Technology and Risk of Abuse of Economic Information (October 1999), PE 168.184.

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. Campbell bases his claims on reports in the American press[6]

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[7]. 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 a committee of inquiry can be set up 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[8] 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

[6] Raytheon Corp Press release, http://www.raytheon.com/sivam/contract.html; *Scott Shane, Tom Bowman*, America's Fortress of Spies, Baltimore Sun, 3.12.1995
[7] European Parliament decision of 5 July 2000, B5-0593/2000, OJ C 121/131 of 24 April 2001.
[8] 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).

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 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, 8. Legal context and protection of privacy and 9. Implications for the EU's external relations. 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 (UKUSA states[9]) 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

[9] See Chapter 5, 5.4.

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.[10] 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

[10] 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' (1996) that 95% of all economic intelligence is derived from open sources (Chapter 2, 'The Role of Intelligence').
http://www.gpo/int/report.html

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 in general only protects nationals within the territory of their own country and other residents of the country concerned (see Chapter 8).

2.5. The operations of certain intelligence services

Public debate has been sparked primarily by the interception operations of the US 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 US 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 UKUSA states

The columns refer to:

Column 1: The country concerned

Column 2: Foreign Communications; all incoming and outgoing civilian, military or diplomatic communications[11]

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

Column 4: Civilian communications

[1]+[1] signifies that communications are intercepted
[1]-[1] signifies that communications are not intercepted

[11] If the intelligence service has access to the relevant cables, it can intercept both incoming and outgoing communications. If the intelligence service targets satellite communications, it has access only to the downlink, but can intercept all the communications it carries, including those not intended for its own territory. Since as a rule the satellite footprints cover the whole of Europe or an even wider area (see Chapter 4, 4.2.5.), satellite communications throughout Europe can be intercepted using receiving stations in one European country.

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[12]

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.

- Although the infrastructure required is costly and complex, communications from a **mobile phone** can be intercepted if the interception station is situated in the same radio cell (diameter 300 m in urban areas, 30 km in the countryside).

- **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.

[12] *Manfred Fink*, Eavesdropping on the economy – Interception risks and techniques – prevention and protection, Richard Boorberg Verlag (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 ocean bed 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 UKUSA 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 small proportion of intra-European Internet communications are routed via the USA[13].

[13] With the aid of a demonstration version of Visual Route, a programme which reveals the route taken by an Internet link, it was shown that a link from Germany to England, Finland or Greece passes via the USA and the UK. A link from Germany to France likewise passes via the UK. Links from Luxembourg to Belgium, Greece, Sweden or Portugal pass via the USA, and to Germany, Finland, France, Italy, the Netherlands or Austria via the switch in London. http://visualroute.cgan.com.hk/

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

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

3.3.1.2. Radio communications[14]

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.

[14] *Ulrich Freyer*, Message transmission technology, Hanser Verlag (2000).

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 **UKUSA states** with terrestrial listening stations is that they can intercept only a very limited proportion of radio communications.

3.3.1.3. Communications transmitted by geostationary telecommunications satellites[15]

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 **UKUSA 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[16]. 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[17].

In addition, surface ships, and in coastal regions, submarines are used to intercept military radio transmissions[18].

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[19]. The satellites cannot be used for the continuous monitoring of civilian radio communications.

---

[15] *Hans Dodel*, Satellite communications, Hüthig Verlag (1999).
[16] Letter from the Minister of State in the German Federal Defence Ministry, Walter Kolbow, to the rapporteur, dated 14 February 2001.
[17] Süddeutsche Zeitung No 80, 5.4.2001, 6.
[18] *Jeffrey T. Richelson*, The U.S. Intelligence Community (1989), 188, 190.
[19] Letter from the Minister of State in the German Federal Defence Ministry, Walter Kolbow, to the rapporteur, dated 14 February 2001.

Alongside these satellites, the USA operates so-called quasi-geostationary SIGINT satellites stationed in a high earth orbit (42 000 km)[20]. 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.

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[21]. However, according to the information available to the rapporteur the automatic recognition to a sufficient degree of accuracy 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[22].

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[23], combined with the evidence given to the Temporary Committee on 21 November 2000 by Mr Ernst

[20] Major *A. Andronov*, Zarubezhnoye voyennoye obozreniye, No 12, 1993, 37-43.
[21] Information supplied privately to the rapporteur (source protected).
[22] Information supplied privately to the rapporteur (source protected).
[23] BverfG, 1 BvR 2226/94, 14 July 1999, paragraph 1.

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 (until May 2001 the FIS was not authorised to intercept foreign cable communications in Germany).

On the basis of differing legal provisions 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 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[24]). 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.

[24] 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; it lies between 0.4 and 5%[25]. 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[26].

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.

[25] Information drawn from the answers given to the Temporary Committee by telecommunications service providers from a number of Member States.
[26] 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[27]

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 roughly 36 000 km – it has a **geostationary** position. Most communications and television satellites are satellites of this type.

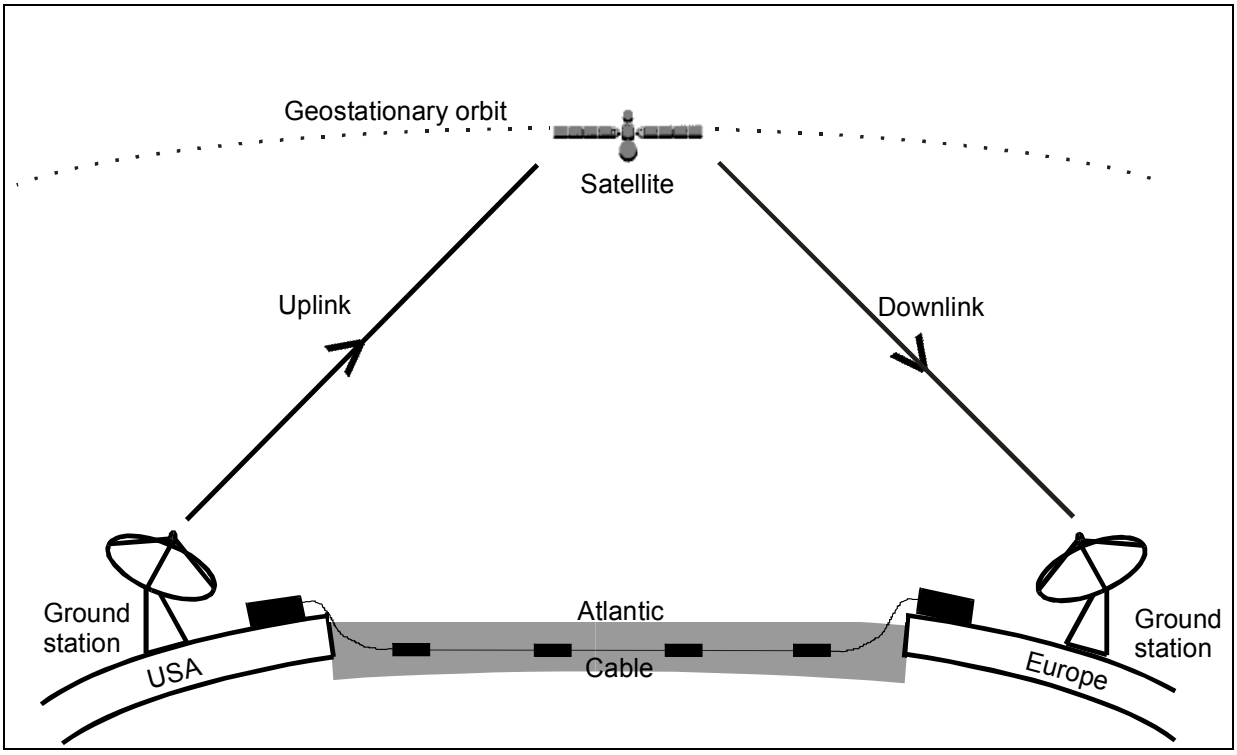
4.2.2. The route followed by signals sent via a satellite communication link

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 satellite telephones 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.

[27] *Hans Dodel*, Satellite communications, Hüthig Verlag (1999), *Georg E. Thaller*, Satellites in Earth Orbit, Franzisverlag (1999)



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[28].

In addition, the far northern areas of the earth are covered by satellites in a highly elliptical orbit (Russian molnyia orbits) in which the satellites are visible to users in the far north for half their orbit. In principle, two satellites can provide full regional coverage[29], which is not feasible from a geostationary position above the equator. In the case of the Russian Molnyia satellites, which have been in service as communications satellites since 1974 (prototype launched in 1964), three equidistant satellites orbit the earth once every 12 hours and thus guarantee continuous transmission of communications[30].

[28] *Georg E. Thaller*, Satellites in Earth Orbit, Franzisverlag (1999).
[29] Cf. *Hans Dodel*, Satellite communications, Hüthig Verlag (1999)
[30] Hompage of the Federation of American Scientists, http://www.geo-orbit.org

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[31].

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[32]

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 20 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 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

[31] *Hans Dodel*, private information.
[32] INTELSAT homepage: http://www.intelsat.com

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[33]

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 international organisation which the government of any country can join. It now has 24 member countries (including Germany) and some 40 users (including France and the UK), 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[34]

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; 4.2.4).

PANAMSAT[35]

PanAmSat was founded in 1988 as a commercial provider of a global satellite system and has its headquarters in the USA. PanAmSat now has a fleet of 21 satellites which provide services such as television, Internet and telecommunications on a worldwide basis, albeit chiefly in the USA.

Telecommunications are transmitted via the C-band and the Ku-band. Of the 21 satellites, seven cover the Atlantic region, two the Pacific region and two the Indian Ocean region. The footprints

[33] INTERSPUTNIK homepage: http://www.intersputnik.com
[34] INMARSAT homepage: http://www.inmarsat.com
[35] PANAMSAT homepage: http://www.panamsat.com

of the remaining satellites cover North and South America. The PanAmSat satellites play only a secondary role in communications in Europe.

4.2.3.2. Regional satellite systems

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[36]

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[37]

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[38]

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.

[36] EUTELSAT homepage: http://www.eutelsat.com
[37] ARABSAT homepage: http://www.arabsat.com
[38] *Hans Dodel*, Satellite communications, Hüthigverlag (1999)

4.2.3.3. National satellite systems[39]

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.

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 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 (ITU) 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. military communications satellites (see Chapter 4.4.3);
- the V-band (46 – 56 GHz) for very small earth stations (VSATs).

4.2.5. Satellite footprints

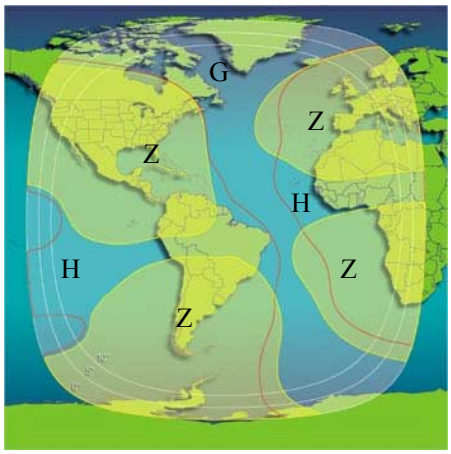
The footprint is the area on the earth covered by a satellite antenna. It may embrace up to 50% of the earth's surface, or, by means of signal focusing, be restricted to small, regional spots.

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

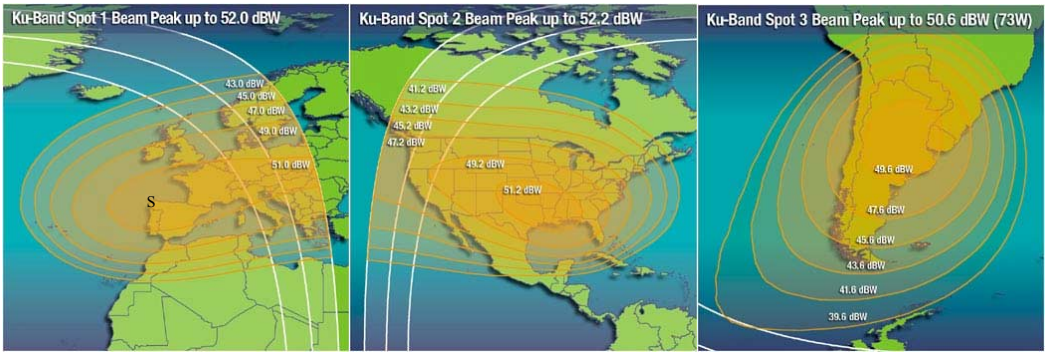
[39] *Hans Dodel* and Internet research

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[40].



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 with a diameter of between 0.5 and 30m 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.

[40] INTELSAT satellite 706, 307°E, footprints taken from the INTELSAT homepage, http://www.intelsat.com

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 antennae 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 antennae, 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 (see also Chapter 5, 5.2.3.).

Today, the typical antennae required for INTELSAT communications in the C-band have a diameter of between 13 and 20 m.

Antennae with a diameter of between 2 and 5 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 0.5 and 3.7 m are adequate (e.g. VSATs from EUTELSAT or INMARSAT).

4.3. Satellite communications for military purposes

4.3.1. General

Communications satellites play an important role in the military sphere as well. Many countries, including the USA, the United Kingdom, France and Russia, operate their own geostationary military communications satellites, with the aid of which independent global communication is possible The USA has stationed one satellite roughly every 10° around the earth in some 32 orbital positions. However, some use is also made of commercial geostationary satellites for the purposes of providing military communications.

4.3.2 Frequencies used for military purposes

The frequency bands used for military communications lie in the range between 4 Ghz and 81 Ghz. The bands typically used by military communications satellites are X-band (SHF - 3-30 Ghz) and the Ka-band (EHF - 20-46 Ghz).

4.3.3. Size of the receiving stations

A distinction must be drawn between mobile stations, which may have a diameter of only a few decimetres, and fixed stations, which generally have a diameter not exceeding 11m. There are, however, two types of antenna (to receive signals from DSCS satellites) with a diameter of 18m.

4.3.4. Examples of military communications satellites

The US **MILSTAR** program (Military Strategy, Tactical and Relay Satellite System), which operates six geostationary satellites worldwide, enables US armed forces to communicate with

each other and with command centres using small earth stations, aircraft, ships and man-packs. Through the link among the satellites themselves worldwide communications availability is guaranteed even if all the US earth stations cease operating.

The **DSCS** (Defense Satellite Communications System) also provides global communications by means of five geostationary satellites. The system is used by the US armed forces and some government agencies.

The British military satellite system **SKYNET** also provides global communications.

The French system **SYRACUSE**, the Italian system **SICRAL** and the Spanish system fly piggy-back on their respective national civilian communications satellites and provide military communications, albeit only on a regional basis, in the S-band.

The Russians guarantee their armed forces' communications by means of transponders in the X-band used by the Molnyia satellites.

NATO operates its own communications satellites (**NATO IIID, IVA** and **IVB)**. The satellites provide voice, telex and data links between military units.

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 UKUSA 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 UKUSA states intercept private and business communications;
- evidence that interception stations operated by the UKUSA 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 UKUSA 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 UKUSA 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.[41]

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 Chapter 4, 4.2.5.).

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

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

- 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 UKUSA 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.

5.1.3. Evidence of a close intelligence association

On the other hand it has not been disclosed whether and to what extent the UKUSA 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 alliance 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, broadcasting organisations 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 at least part of the technical work of interception. In the case of the stations run by the USA, for example, operations are carried out jointly with the NSA by the Naval Security Group (NAVSECGRU), the United States Army Intelligence and Security Command (INSCOM) or the Air Intelligence Agency (AIA). In the British stations, the British intelligence service GCHQ operates the installations jointly with the Royal Air Force (RAF). 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 interception 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 satellites;
- receiving station for spy satellites (pictures, radar);
- receiving station for 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, the diameter of the antennae gives some clues as to their purpose. 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 15-20 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.

In the sphere of military communications as well, command centres have two types of antenna with a diameter of roughly 18 m (AN/FSC-78 and AN/FSC-79). However, most antennae for military communications have a much smaller diameter, since they must be transportable (tactical stations).

In view of the nature of the signals transmitted back to the station (high degree of focusing and high frequency), earth stations for SIGINT satellites need only small antennae. This also applies to antennae which receive signals from spy satellites.

If a site houses two or more satellite antennae with a diameter of at least 18 m, one of its tasks is certainly that of intercepting civilian communications. In the case of a station housing US forces, one of the antennae may also be used to receive military communications.

5.2.4. Criterion 4: Evidence from official sources

Official descriptions of the tasks of some stations have been published. In that connection governments and military units are regarded as official sources. If this criterion has been met, the others become superfluous.

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[42], Richelson[43], Campbell[44]) declassified documents[45], the homepage of the Federation of American Scientists[46] and operators' homepages[47] (NSA, AIA, etc.) and other Internet publications were analysed. In the case of the New Zealand station in Waihopai, the New Zealand Government has drawn up an official description of its tasks[48]. 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. In principle, different, overlapping beams

---

[42] *Nicky Hager*: Exposing the Global Surveillance System http://www.ncoic.com/echelon1.htm
Nicky Hager: Secret Power. New Zealand's Role in the International Spy Network, Craig Potton Publishing (1996).
[43] *Jeffrey T. Richelson*, Desperately Seeking Signals, The Bulletin of the Atomic Scientists, Vol 56, No. 2, 47-51, http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html
Richelson, T. Jeffrey, The U.S. Intelligence Community, Westview Press (1999).
[44] *Duncan Campbell*, 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, Part 4/5, in STOA (Ed.). Development of Surveillance Technology and Risk of Abuse of Economic Information, (October 1999), PE 168.184 http://www.europarl.eu.int/dg4/stoa/en/publi/pdf/98-14-01-2en.pdf
Duncan Campbell: Inside Echelon, 25.7.2000, http://www.heise.de/tp/deutsch/special/ech/6928/1.html
Campbell, Duncan: Interception Capabilities 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
[45] *Jeffrey T. Richelson*: 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
[46] Federation of American Scientists (FAS), http://www.fas.org/irp/nsa/nsafacil.html.
[47] Military.com; *.mil-Homepages.
[48] Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet, Securing our Nation's Safety (2000), http://www.dpmc.govt.nz/dess/securingoursafety/index.html

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, although this leads to a deterioration in the signal-noise ratio.

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[49], 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 at least 30 m for the first INTELSAT generation and more than 15 to 18 m for later generations. The official descriptions of the tasks of some of the stations have been cited as evidence of their role in interception operations.

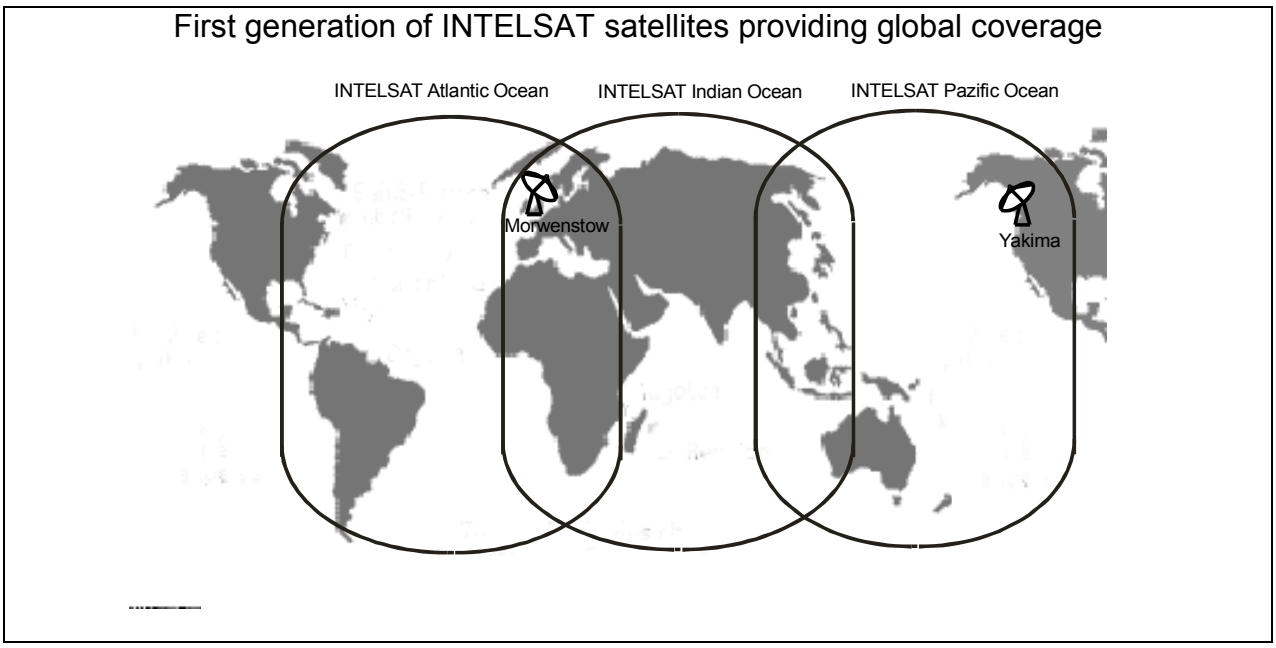
5.3.2.1. The parallel between the development of INTELSAT and the building of stations

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 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 global 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.

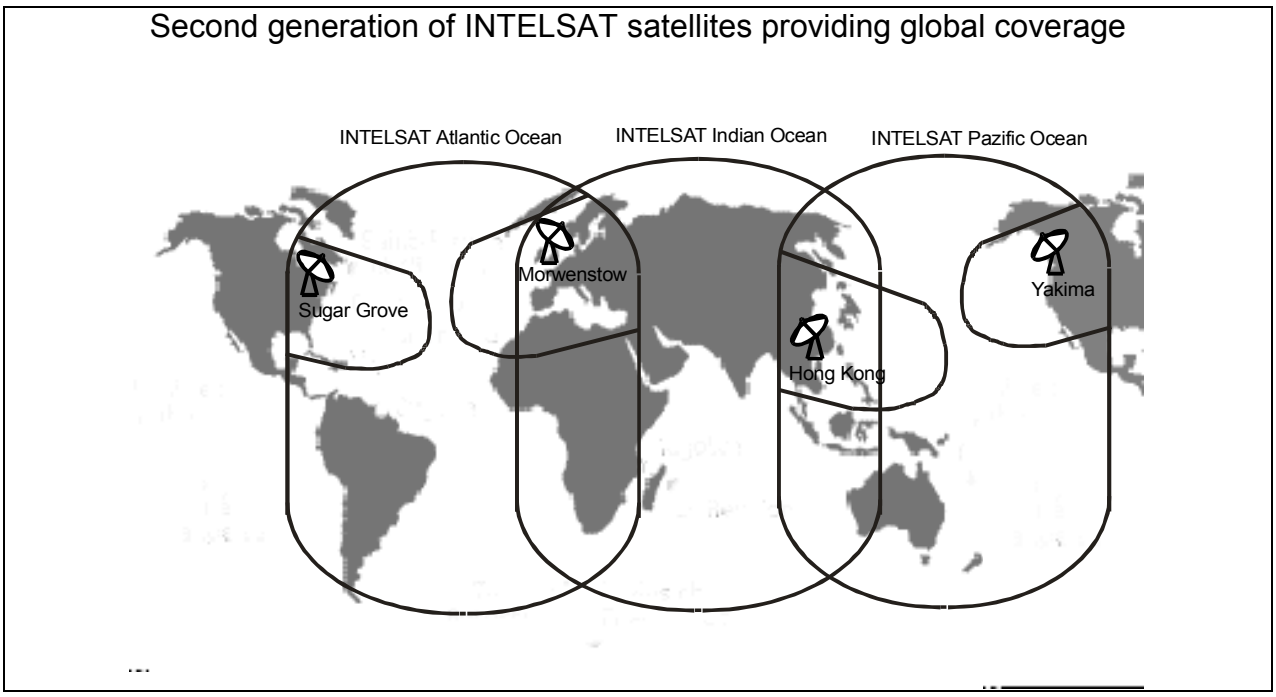
[49] Abbreviations used: NAVSECGRU: Naval Security Group, INSCOM: United States Army Intelligence And Security Command, AIA: Air Intelligence Agency, IG: Intelligence Group, IS: Intelligence Squadron, IW: Intelligence Wing, IOG: Information Operation Group, MIG: Military Intelligence Group.



In the early 1970s 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.

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.



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, on the basis of the information available, it is difficult to document a link with the development of further stations and/or the introduction of new satellite antennae.

Since it is equally 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 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, and although there is no other clear evidence underpinning the assumption, 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, 5.2.) and stations whose role cannot definitely 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 the 1970s, 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 normal 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 greater 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[50].
In addition, Sugar Grove is situated close (60 miles) to the normal satellite receiving station in Etam.

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 21 satellite antennae, three 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.

[50] '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 12 of which have a diameter of more than 20 m. At least one of the large antennae, although certainly not all, is a receiving antenna for military communications (AN/FSC-78). The British and Americans work together at Menwith Hill. The US 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 interception station for 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, four satellite antennae, of the same size (diameter of roughly 20 m) are trained on satellites above the Indian Ocean and the Pacific.
According to statements made under oath in the Australian Parliament by an expert, transmissions from civilian telecommunications satellites are intercepted at Geraldton[51].

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[52].
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 as the site for an HFDF antenna. It is manned by Japanese and Americans. The US 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.

---

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

Waihopai, New Zealand (173°O, 41°S)[53]
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 antennae are trained on INTELSAT 701 in orbit above the Pacific. Official information released by the GCSB (General Communications Security Bureau) Waihopai's task is to intercept transmissions from communications satellites and to decrypt and process the signals.[54]

Since the station has only two satellite antennae, the New Zealand secret service can intercept only a small proportion of communications in the Pacific region. To serve any purpose, therefore, the station must work jointly with other stations in the region. Hager often names Geraldton in Australia as Waihopai's 'sister station'.[55]

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 US 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)
At present roughly 750 Americans work at the station near Bad Aibling. INSCOM (66th IG, 718th IG) which has the command, NAVSECGRU, 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 Common, Support to DoD and Unified Commands, Medium and

[53] Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet 'Securing our Nation's Safety', December 2000, http://www.dpmc.govt.nz/dess/securingoursafety/index.html
[54] Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet: 'Securing our Nations Safety', December 2000, http://www.dpmc.govt.nz/dess/securingoursafety/index.html: 'In 1989, [...] the GCSB opened its satellite communications interception station at Waihopai, near Blenheim. [...] The signals intelligence is obtained from a variety of foreign communications and other non-communications signals, such as radar. The GCSB not only intercepts the signals, it also processes, decrypts or decodes and/or translates the information the signals contain before passing it on as a report to the appropriate Minister or government department.'
[55] *Nicky Hager,* Secret Power. New Zealands´s Role in the International Spy Network, Craig Potton Publishing (1996), 182

Longhand Common HF & Satellite, Communication Physics Research, Test and Evaluate Common Equipment'. According to Richelson, Bad Aibling is an earth station for SIGINT satellites and a listening station for transmissions from Russian telecommunications satellites. In accordance with a Department of Defense decision, the station is to be closed on 30 September 2002. Personnel will be transferred to other units.[56]

Ayios Nikolaos, Cyprus (32°O, 35°N)
Ayios Nilolaos on Cyprus is a British station. The station, which has 14 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 four satellite antennae, two of which have a diameter of roughly 15 m.

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.

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 at least six 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.

Medina Annex, Texas, USA (98°W, 29°N)
Like Kunia, Medina, which was established in 1993, is an 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.

[56] Announcement of 31 May 2001 on the INSCOM homepage, http://www.vulcan.belvoir.army.mil/bas_to_close.asp

Fort Meade, USA (76°W, 39°N)
Ford Meade 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 20 m. They are stations which are operated by the Americans or British or where American or British servicemen carry out intelligence activities.

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. According to official information, some of these stations have the task of intercepting transmissions from communications satellites.

4. The information regarding stations contained in the declassified documents 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[57]

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.

[57] *Christopher Andrew*, The making of the Anglo-American SIGINT Alliance in *Hayden B. Peake, Samuel Halpern* (Eds.), In the Name of Intelligence. Essays in Honor of *Walter Pforzheimer,* NIBC Press (1994), 95 -109

It was the Americans who instigated the establishment of a SIGINT alliance at a meeting with the British in London in August 1940[58]. In February 1941, US codebreakers delivered a cipher machine (PURPLE) to the United Kingdom. Cooperation in the sphere of codebreaking began in spring 1941[59]. 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, US codebreakers from the Naval SIGINT Agency began work in the United Kingdom[60]. 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[61].

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[62].

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[63]. Immediately thereafter, negotiations on an

---

[58] *Christopher Andrew,* The making of the Anglo-American SIGINT Alliance, ibidem, 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'. (quoted from COS (40)289, CAB 79/6, PRO. *Smith*, The Ultra Magic Deals, 38, 43-4. *Sir F.H. Hinsley*, et al., British Intelligence in the Second World War, Vol. I, 312-13).

[59] *Christopher Andrew* The making of the Anglo-American SIGINT Alliance, ibidem,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'.

[60] *Christopher Andrew,*The making of the Anglo-American SIGINT Alliance, ibidem, 100 (*Sir F.H. Hinsley*, et al., British Intelligence in the Second World War, Vol. II, 56)

[61] *Christopher Andrew,*The making of the Anglo-American SIGINT Alliance, ibidem, 101 (*Sir F.H. Hinsley*, et al., British Intelligence in the Second World War, Vol. II, 48)

[62] *Christopher Andrew,*The making of the Anglo-American SIGINT Alliance, ibidem, 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

[63] *Harry S. 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.' (quoted from *Bradley F.*

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[64].

5.4.2. Evidence for the existence of the agreement

5.4.2.1. 1999/2000 annual report of the UK Intelligence and Security Committee

For a long time, the signatory states refused officially to acknowledge the existence of the UKUSA Agreement. However, the annual report of the Intelligence and Security Committee, the UK's parliamentary monitoring body, refers explicitly to the agreement: 'The quality of intelligence gathered clearly reflects the value of the close co-operation under the UKUSA agreement. A recent illustration of this occurred when the US National Security Agency's (NSA) equipment accidentally failed and for some three days US customers, as well as GCHQ's normal UK customers, were served directly from GCHQ'.[65]

5.4.2.2. Publication of the New Zealand Department of the Prime Minister

A publication of the New Zealand Department of the Prime Minister from the year 2000, dealing with the management of the New Zealand's security and intelligence services, also refers clearly to the agreement: .'The operation of the GCSB is directed solely by the New Zealand Government. It is, however, a member of a long-standing collaborative international partnership for the exchange of foreign intelligence and the sharing of communications security technology. The other members of the partnership are the USA's National Security Agency (NSA), the UK's Government Communications Headquarters (GCHQ) Australia's Defence Signals Directorate (DSD), and Canada's Communications Security Establishment (CSE). New Zealand gains considerable benefit from this arrangement, as it would be impossible for New Zealand to generate the effectiveness of the five nation partnership on its own'.[66]

Moreover, there is further evidence of the agreement's existence.

Smith, The Ultra-Magic Deals and the Most Secret Special Relationship (Novato, Ca: Presidio 1993))

[64] *Christopher Andrew*, The making of the Anglo-American SIGINT Alliance in Hayden, H. Peake and Samuel Halpern Eds, In the Name of Intelligence. Essays in Honor of Walter Pforzheimer (NIBC Press 1995) 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.

[65] Intelligence and Security Committee Annual Report 1999-2000. Presented to Parliament by the Prime Minister by Command of Her Majesty, November 2000, 8, 14

[66] Domestic and External Secretariat of the Department of the Prime Minister and Cabinet of New Zealand, Securing our Nation's Safety. How New Zealand manages its security and intelligence agencies (2000).

5.4.2.3. The Navy acronym list

According to the US Navy[67], UKUSA stands for 'United Kingdom-USA' and refers to a '5-nation SIGINT agreement'.

5.4.2.4. 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[68].

5.4.2.5. 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.

5.4.2.6. 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[69].

5.4.2.7 Letter from the former Head of HCHQ, Joe Hooper

The former Head of GCHQ, Joe Hooper, refers to the UKUSA Agreement in a letter of 22 July 1969 to the former Director of the NSA, Marshall S. Carter.

5.4.2.8. 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 US 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.

---

[67] '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

[68] *Martin Brady*, Head of the DSD, letter of 16.3.1999 to Ross Coulthart, Sunday Program Channel 9

[69] *Christopher Andrew* 'The growth of the Australian Intelligence Community and the Anglo-American Connection', 223-4.

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).[70] 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 intelligence satellites.[71] Following our conversation with Jeffrey Richelson in Washington he forwarded further declassified documents to the Temporary Committee. Those relevant to our investigations have been taken into account here.

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, 2b, 4, 10 and 16)

In National Security Council Intelligence Directive 9 (NSCID 9) of 10 March 1950[72] 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, 29.12.1952)[73] expressly states that the FBI alone is responsible for internal security.

The Department of Defense (DoD) Directive of 23 December 1971[74] 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 Defence;
- 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 1971 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[75], Gen. Michael Hayden, the NSA Director, defined the NSA's tasks as follows:

---

[70] *Jeffrey T.Richelson*, The National Security Agency Declassified, National Security Archive Electronic Briefing Book No 24, George Washington University http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html
[71] *Jeffrey T. Richelson,* The National Security Agency Declassified, National Security Archive Electronic Briefing Book No 24, George Washington University http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB35/index.html
[72] Document 1. NSCID 9, 'Communications Intelligence,' March 10 1950.
[73] Document 2b. National Security Council Intelligence Directive No 9, Communications Intelligence, December 29 1952
[74] Document 4. Department of Defense Directive S-5100.20, 'The National Security Agency and the Central Security Service,' December 23 1971

- 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[76], 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)[77]

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.[78]

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

The NAVSECGRU Instructions C5450.48A[79] 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[80] the Air Intelligence Agency (AIA), Detachment 2 and 3, is mentioned under the heading 'Activation of ECHELON Units'.

---

[75] Document 16. Statement for the Record of NSA Director Lt Gen Michael V. Hayden, USAF before the House Permanent Select Committee on Intelligence, April 12 2000.
[76] Document 10. Farewell from Vice Admiral William O. Studeman to NSA Employees, April 8 1992.
[77] Document 7. United States Signals Intelligence Directive [USSID] 18, 'Legal Compliance and Minimization Procedures,' July 27 1993.
[78] Document 2a. Memorandum from President Harry S. Truman to the Secretary of State, the Secretary of Defense, Subject: Communications Intelligence Activities, October 24 1952.
Document 2b. National Security Council Intelligence Directive No. 9, Communications Intelligence, December 29 1952.
[79] Document 9. NAVSECGRU Instruction C5450.48A, Subj: Mission, Functions and Tasks of Naval Security Group Activity (NAVSECGRUACT) Sugar Grove, West Virginia, September 3 1991.
[80] Document 12. 'Activation of Echelon Units,' from History of the Air Intelligence Agency, 1 January - 31 December 1994, Volume I (San Antonio, TX: AIA, 1995).

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, new documents)

- Sugar Grove, West Virginia, named as SIGINT station in the NAVSECGRU Instructions C5450.48A[81]
- Misawa Air Base, Japan, named as SIGINT station in History of the Air Intelligence Agency – 1 January to 31 December 1994[82] and in description of the activities of the Naval Security Group in Department of the Navy documents[83]
- Sabana Seca in Puerto Rico, ibid. and in description of the activities of the Naval Security Group in Department of the Navy documents[84]
- Guam, named as SIGINT station, ibid.
- Yakima, Washington, named as SIGINT station, 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[85]
- Menwith-Hill, United Kingdom, description of the activities of the Naval Security Group in Department of Navy documents[86]
- Bad Aibling, Germany, description of the activities of the Naval Security Group in Department of Navy documents[87]
- Medina, Texas, description of the activities of the Naval Security Group in Department of Navy documents[88]
- Kunia, Hawaii, description of the activities of the Naval Security Group in Department of Navy documents[89]

5.5.2.6. Protection of the privacy of US citizens (Documents 7, 7 a to f, 9, 11 and 16)

The NAVSECGRU Instructions C5450.48A state that the privacy of citizens must be protected[90].

Various documents state that the privacy of US 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.[91]

---

[81] Document 9. NAVSECGRU Instruction C5450.48A, Subj: Mission, Functions and Tasks of Naval Security Group Activity (NAVSECGRUACT) Sugar Grove, West Virginia, September 3, 1991.
[82] Document 12. 'Activation of Echelon Units,' from History of the Air Intelligence Agency, 1 January - 31 December 1994, Volume I (San Antonio, TX: AIA, 1995).
[83] Department of the Navy, Naval Security Group Instruction C5450.32E, 9.5.1996
[84] Naval Security Group Instruction C5450.33B, 8.8.1996
[85] COMINT report by the NSA from Fort George G. Meade, Maryland of 31 August 1972
[86] Department of the Navy, Fact and Justification Sheet for the Establishment of U.S. Naval Security Group Activity of 23.2.1995 and Department of the Navy, Naval Security Group Instruction C5450.62, 30.1.1996
[87] Department of the Navy, Naval Security Group Instruction C5450.63, 25.10.1995
[88] Department of the Navy, Naval Security Group Instruction C5450.60A, 8.4.1996
[89] Naval Security Group Instruction C5450.55B, 8.8.1996
[90] Document 9. NAVSECGRU Instruction C5450.48A, Subj: Mission, Functions and Tasks of Naval Security Group Activity (NAVESCGRUACT) Sugar Grove, West Virginia, 3 September 1991
[91] 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

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

The Department of Defense Directive of 23 December 1971[92] provides precise definitions of SIGINT, COMINT, ELINT and TELINT, as does the National Security Council Intelligence Directive No 6 of 17 February 1972.[93]

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. Further stations at which the Naval Security Group is active are named without being identified as SIGINT stations.
9. 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.

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.

[92] Document 4. Department of Defense Directive S-5100.20, 'The National Security Agency and the Central Security Service,' December 23 1971

[93] Document 5a. NSCID 6, 'Signals Intelligence,' February 17 1972.

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 the book 'Secret Powers – New Zealand's role in the international spy network', published in 1996 by the New Zealand author Nicky Hager.

He draws on interviews with more than 50 persons who were employed by the New Zealand intelligence service, GCSB, or otherwise involved in intelligence activities. He also analysed a wide range of documents from national archives, newspapers and other published sources. According to Hager, the global interception system is referred to as ECHELON, and the network computers as ECHELON Dictionaries.

According to Hager, the origins of cooperation between intelligence services under the UKUSA Agreement 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 the core activity of the **current** system. The interception by ground stations of messages sent via Intel satellites – the first global satellite communication system[94] - 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[95], 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.

In his statement to the Temporary Committee, made on 24 April 2001, Hager emphasised that the interception system was not all-powerful. Since the limited resources had to be used as effectively as possible, not all communications could be intercepted, but rather only those likely to offer up important information. For that reason, the communications targeted were those of political and diplomatic interest. If communications were intercepted with a view to obtaining economic intelligence, the information concerned the macro - rather than the microeconomic sphere.

[94] Intelsat homepage, http://www.intelsat.int/index.htm
[95] Inmarsat homepage, http://www.inmarsat.org/index3.html

As far as the interception system's operating methods were concerned, each partner state had its own list of search words on the basis of which communications were intercepted. In addition, however, communications were screened for keywords entered into the system by the USA using 'dictionary managers'. The British therefore had no control over the screening process and had no idea what information was collected in Morwenstow, since it was forwarded directly to the USA.

In that connection, Hager emphasised the risk posed to continental Europe by the British interception stations. Citing several examples, he pointed out that the UKUSA partner states were spying on allies and trading partners in the Pacific. The only countries not being spied on were the UKUSA partner states themselves. In Hager's view, like their New Zealand counterparts the British secret services would probably be very loath to call the UKUSA partnership into question by refusing to cooperate and intercept communications originating from continental Europe. There would be no reason for the United Kingdom to forfeit information of interests to its intelligence services, and, since that information would always remain secret, espionage under the UKUSA Agreement would not rule out an official policy of loyalty vis-à-vis Europe.

5.6.2. Duncan Campbell

In his many publications the British journalist Duncan Campbell draws on the work of Hager and Richelson, on conversations with former intelligence service staff and on other research. According to his statements, ECHELON is part of the global system which intercepts and analyses international satellite communications. Each partner state uses 'dictionary' computers which screen the intercepted messages for keywords.

In STOA Study 2/5 of 1999, which provides an in-depth analysis of the technical aspects, Campbell describes 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.’ [96]

In his statement to the Temporary Committee, made on 22 January 2001, Campbell expressed the view that the USA used its intelligence services to help US firms win contracts. Relevant information was passed on to firms via the CIA with the assistance of the Advocacy Center and the Office of Executive Support in the Department of Commerce. In support of this argument he put forward documents providing evidence of intervention by the Advocacy Center to the benefit of US firms; moreover, much of the information concerned can be found on the homepage of the Advocacy Center.[97] The claim that the success of the Advocacy Center is based on the interception of communications is speculation and is not supported by the documents.

---

[96] *Duncan Campbell*, Inside ECHELON. The history, structure and function of the global surveillance system known as ECHELON, 1

[97] Homepage of the Advocacy Center, http://www.ita.doc.gov/td/advocacy/index.html
In the course of his visit to Washington DC your rapporteur wanted to give the Advocacy Center an opportunity to respond to these accusations. However, a pre-arranged meeting was cancelled by the Department of Commerce at short notice.

Campbell emphasised that the interception capabilities of several European countries (e.g. Switzerland, Denmark, France) had increased substantially in recent years. The intelligence sector had also seen an expansion in bilateral and multilateral cooperation.

5.6.3. Jeff Richelson

The US author, Jeffrey Richelson, a former member of the National Security Archives, has made available on the Internet 16 previously classified documents which give an insight into the inception, development, management and remit of the National Security Agency[98].

In addition, he is the author of various books and articles on the intelligence activities of the USA. In his work he draws on many declassified documents, the research carried out by Hager and his own research. During his meeting with the delegation from the Temporary Committee, held in Washington DC on 11 May 2001, he stated that ECHELON referred to a computer network used to filter data which was then exchanged between intelligence services.

In his 1985 book 'The Ties That Bind'[99] he describes in detail the negotiations which led up to the signing of the UKUSA Agreement and the activities under that agreement of the secret services of the USA, the United Kingdom, Canada, Australia and New Zealand.

In his very comprehensive 1999 book 'The US Intelligence Community'[100] he gives a survey of the USA's intelligence activities and describes the organisational structure of the intelligence services and their methods of collecting and analysing information. In Chapter 8 of the book he examines in detail the SIGINT capabilities of the intelligence services and describes some earth stations. In Chapter 13 he outlines the USA's relations with other intelligence services, for example under the UKUSA Agreement.

In his article entitled 'Desperately Seeking Signals'[101], which appeared in 2000, he gives brief details of the substance of the UKUSA Agreement, names installations used to intercept transmissions from communications satellites and outlines the scope for and the limits on the interception of civilian communications.

5.6.4. James Bamford

US author James Bamford, whose work is based both on archive research and the questioning of intelligence service staff, was one of the first people to tackle the subject of the MSA's SIGINT activities As long ago as 1982 he published the book 'The Puzzle Palace'[102], chapter 8 of which, entitled 'Partners', describes the UKUSA Agreement in detail. According to his new book, 'Body of Secrets'[103], which builds on the findings outlined in 'The Puzzle Palace', the computer network linking the intelligence services is known as 'Platform'. ECHELON is the name of the software

---

[98] *Jeffrey T. Richelson*, The National Security Agency Declassified, National Security Archive Electronic Briefing Book No 24, George Washington University, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html
[99] *Jeffrey T. Richelson, Desmond Ball,* The Ties That Bind, Boston UNWIN HYMAN (1985)
[100] *Jeffrey T. Richelson,* The U.S. Intelligence Community[4], Westview Press (1999)
[101] *Jeffrey T. Richelson,* Desperately Seeking Signals, The Bulletin of the Atomic Scientists, Vol. 56, No. 2/2000,
[102] *James Bamford,* The Puzzle Palace, Inside the National Security Agency, America's most secret intelligence organization (1983)
[103] *James Bamford,* Body of Secrets. Anatomy of the Ultra-Secret National Security Agency. From the Cold War Through the Dawn of a New Century, Doubleday Books (2001)

used in all the relevant stations, providing for uniform processing of data and direct access to the data held by other intelligence services[104]. In the subsequent chapters, however, he also uses the term ECHELON to denote the interception system set up under the UKUSA Agreement.

In 'Body of Secrets', and in the chapter of most relevance to the work of the Temporary Committee, entitled 'Muscle', Bamford gives a historical survey of the development of communications surveillance by the NSA and describes the scope of the system, the way the UKUSA partnership operates and its objectives. He emphasises that, according to interviews conducted with dozens of current and former NSA employees, the NSA is at present not involved in the work of gathering competitive intelligence.

He confirmed this statement when giving evidence to the Temporary Committee on 23 April 2001. The NSA could only be given the task of gathering competitive intelligence on the basis of a clear political decision taken at the very highest level, a decision which has thus far not been taken. In the course of 20 years' research, Bamford had never uncovered evidence of the NSA passing on intelligence to US firms, even though it intercepts communications from private firms, for example with a view to monitoring compliance with embargoes.

According to Bamford, the main problem for Europe is not the issue of whether the ECHELON system steals firms' business secrets and passes them on to competitors, but rather that of the violation of the fundamental right to privacy. In 'Body of Secrets' he describes in detail how the protection of 'US persons' (i.e. US citizens and persons legally resident in the USA) has developed and makes clear that at least internal restrictions have been laid down in respect of other UKUSA residents. At the same time, he points out that other persons enjoy no protection, that there is no requirement to destroy data concerning such persons, and that the NSA's data storage capacities are unimaginably huge.

However, Bamford also emphasises the limits of the system, which stem from the fact that, firstly, only a small proportion of international communications are now transmitted via satellites - transmissions via fibreoptic cable are much more difficult to intercept - and, secondly, that the NSA has only limited capacities when it comes to the final analysis of intercepted communications. Moreover, those capacities must be set against an ever-increasing volume of communications, transmitted in particular via the Internet.

5.6.5. Bo Elkjaer and Kenan Seeberg

These two Danish journalists told the Temporary Committee on 22 January 2001 that ECHELON was already very advanced in the 1980s. Denmark, which greatly expanded its interception capabilities in the 1990s, has been cooperating with the USA since 1984.

Echoing their article in Ekstra Bladet[105], in which they referred to an illustrated lecture (25 slides) given by an unnamed officer of the 544th Intelligence Group of the Air Intelligence Agency, they claimed that various NGOs (including the Red Cross) were also ECHELON targets.

---

[104] *James Bamford*, Body of Secrets, Anatomy of the Ultra-Secret National Security Agency, From the Cold War Through the Dawn of a New Century, Doubleday Books (2001), 404.

[105] *Bo Elkjaer, Kenan Seeberg*, ECHELON singles out the Red Cross, A bombshell in the surveillance scandal: The organization is a possible surveillance target, Ekstra Bladet, Denmark, 8.3.2000, http://cryptome.org/echelon-

5.7. Statements by former intelligence service employees

5.7.1. Margaret Newsham (former NSA employee)[106]

Margaret Newsham 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 1981 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 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[107], 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.

During his meeting with the committee delegation in Washington DC Madsen expressed particular concern at the risks to the privacy of European citizens posed by the global espionage system.

5.7.3. Mike Frost (former Canadian secret service employee)

Mike Frost worked for more than 20 years for the CSE, the Canadian secret service[108]. The listening post in Ottawa was just one part of a worldwide network of spy stations.[109] 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.[110] 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

---

red.htm

[106] *Bo Elkjaer, Kenan Seeberg*, ECHELON was my baby – Interview with Margaret Newsham, Ekstra Bladet, 17.1.1999

[107] NBC TV interview '60 Minutes', 27.2.2000; http://cryptome.org/echelon-60min.htm

[108] Communication Security Establishment, subordinate to the Canadian Ministry of Defense, engaged in SIGINT

[109] NBC TV interview '60 Minutes', 27.2.2000; http://cryptome.org/echelon-60min.htm

[110] *Florian Rötzer*, Die NSA geht wegen ECHELON an die Öffentlichkeit; http://www.heise.de/bin/tp/issue/download.cgi?artikelnr=6633&rub_ordner=special

communications, the computer had found the keyword and reproduced the conversation. The analyst was unsure and therefore recorded her personal details.[111]

The intelligence services of the UKUSA states 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.[112]

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 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.[113]

5.8. Information from government sources

5.8.1. USA

James Woolsey, the former director of the CIA, said at a press conference[114] 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.

5.8.2. UK

Answers to various questions in the House of Commons[115] 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[116], which provides the chief of station,[117] as a communications facility.[118] 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

[111] NBC TV interview '60 Minutes', 27.2.2000; http://cryptome.org/echelon-60min.htm
[112] Interview on the Australian Channel 9 on 23.3.1999; http://www.geocities.com/CapitolHill/Senate/8789/sunday1.htm
[113] *Jim Bronskill*, Canada a key snooper in huge spy network, Ottawa Citizen, 24.10.2000, http://www.ottawacitizen.com/national/990522/2630510.html
[114] *James Woolsey*, Remarks at the Foreign Press Center, Transcript, 7.3.2000, http://cryptome.org/echelon-cia.htm
[115] Commons Written Answers, House of Commons Hansard Debates
[116] 12.7.1995.
[117] 25.10.1994
[118] 3.12.1997

present on the site.[119] The presence of US military personnel is governed by the North Atlantic Treaty and special confidential[120] administrative arrangements appropriate to the relationship which exists between the governments of the UK and the USA for the purposes of common defence.[121] 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.[122]

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.[123]

5.8.3. Australia[124]

Martin Brady, Director of the Australian intelligence service DSD[125], 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.[126]

5.8.4. New Zealand

As already outlined under 5.4.2.2. above, a document published by the New Zealand Department of the Prime Minister in 2000, which deals with the role of the national security and intelligence services refers explicitly to the parnership between the intelligence services of the USA, the UK, Canada, Australia and New Zealand and emphasises the benefits for New Zealand[127].

5.8.5. 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.[128] In it, the Netherlands Government takes the view that, although

---

[119] 12.5.2000
[120] 12.7.1995
[121] 8.3.1999, 6.7.1999
[122] 3.12.1997
[123] Intelligence and Security Committee (UK), Annual Report 1999-2000, para. 14, presented to the Commons by the Prime Minister in November 2000.
[124] *Martin Brady*, Director of the DSD, letter of 16.3.1999 to Ross Coulthart, Sunday Program Channel 9 http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp; http://sunday.ninemsn.com/01_cover_stories/article_335.asp
[125] Defence Signals Directorate, Australian intelligence service engaged in SIGINT
[126] 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
[127] Domestic and External Secretariat of the Department of the Prime Minister and Cabinet of New Zealand, Securing our Nation's Safety. How New Zealand manages its security and intelligence agencies (2000)
[128] Brief aan de Tweede Kamer betreffende 'Het grootschalige afluisteren van moderne telecommunicatiesystemen', 19.1.2001

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.

5.8.6. 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.[129] 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.

5.9. Questions to the Council and Commission

On 17 February 1998 the MEP Elly Plooj-van Gorsel[130] tabled a first comprehensive question to the Council on the STOA report and the existence of a global inception system, operated by the USA and with the involvement of the United Kingdom, and on any resulting damage to the commercial interests of European firms. Many further questions on this topic followed.[131] The Council Presidency replied that the Council itself had no relevant information, that it was not involved in such matters and could therefore give no replies.

The similar questions to the European Commission[132] received the following response from that institution: it was aware of the report, but there was no evidence that a Member State had violated the EC Treaty in that respect and no complaints had been submitted.[133] However, the Commission was adopting a vigilant approach, would defend all Community interests and would make further efforts to improve the security of its data network.[134] At the plenary sitting of

[129] *Francesco Sorti*, Dossier esclusivo. Caso ECHELON. Parla Luigi Ramponi. Anche i politici sapevano, Il mondo, 17.4.1998

[130] Written Question P-0501/98 by Elly Plooij-van Gorsel (ELDR) to the Council (17.1.1998). On 14.5.1997 Jonas Sjöstedt had tabled a question (H-0330/97) on the Council Resolution of 17.1.1995 on the lawful interception of telecommunications, raising the issue of a link with ECHELON. No reply was given to this last part of the question. The questions tabled by Mihail Papayannakis (G-004/98) and Nel van Dijk (H-0035/98) on British espionage activities were answered, on 18.2.1998, to the effect that the activities of intelligence services were exclusively a matter for national authorities and that the Council had no information whatsoever about such activities.

[131] Written Question E-0499/98 to the Council by Elly Plooij-van Gorsel (ELDR) (27.2.1998), Written question E-1775/98 to the Council by Lucio Manisco (GUE/NGL) (8.6.1998), Oral Question H-1086/98 to the Council by Patricia McKenna (16.12.1998), Oral Question H-1172/98 to the Council by Patricia McKenna (13.1.1999), Oral Question H-1172/98 to the Council by Inger Schörling (13.1.1999), Oral Question H-0526/99 to the Council by Pernille Frahm (6.10.1999), Oral Question H-0621/99 to the Council by Lorna Dybkjaer (19.11.1999), etc:

[132] Written Question E-1039/98 by Nel van Dijk (V) (15.5.1998), Written Question E-1306/98 by Cristiana Muscardini (NI) (15.6.1998), Written Question E-1429/98 by Daniela Raschhofer (NI) (25.6.1998), Written Questions E-1987/98 and E-2329/98 by Nikitas Kaklamanis (3.9.1998, 25.9.1998), Written Question E-1776/98 by Lucio Manisco (GUE/NGL), Written Question E-3014/98 by Paul Lannoye (V) (6.11.1998), Oral Question H-0547/99 by Pernille Frahm, Oral Question H-1067/98 by Patricia McKenna (V) (16.12.1998), Oral Question H-1237/98 by Inger Schörling (13.1.1999), Oral Question H-0092/99 by Ionnis Theonas (13.1.1999), Oral Question H-0547/99 by Pernille Frahm (6.10.1999), Oral Question H-0622/99 by Lone Dybkjaer (17.12.1999), etc.

[133] Commissioner Bangemann replying on 25.9.1998, on behalf of the Commission, to Written Question E-1776/98 by Lucio Manisco (GUE/NGL).

[134] Commission President Santer replying on 3.9.1998, on behalf of the Commission, to Written Question E-

14 September 1998, Commissioner Bangemann stated that the Commission had not received from the Member States, members of the public or firms evidence that the interception system existed in the form suggested. 'If the system existed in such a form, that would naturally represent a blatant violation of rights, the individual rights of citizens, and of course an attack on the security of the Member States. That is absolutely clear. The Council, and naturally the Commission and Parliament as well, would have to respond the instant something of that kind was officially confirmed'. The Commission would then 'be using all its powers to persuade the Member States not to obtain information illegally in this way'.[135]

5.10. Parliamentary reports

5.10.1. 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.

5.10.2. 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[136]. At the meeting held on 28 November 2000 the rapporteur, Arthur Paecht, presented the report's findings to the Temporary Committee.

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

---

1987/98.

[135] Debates of the European Parliament, sitting of Monday, 14 September 1998, Item 7, Transatlantic relations/ECHELON system.

[136] 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.

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.

5.10.3. Report of the Italian Parliament's Committee on Intelligence and Security Services and State Security

In Italy the parliamentary Committee on Intelligence and Security Services drew up a report entitled 'The role of the intelligence and security services in the ECHELON case'[137], which was forwarded to the President of the Italian Parliament on 19 December 2000.

The conclusions concerning the existence of a system named ECHELON are vague. According to the report, 'during the hearings in committee the existence of an integrated interception system of that name, operated by the five signatory states to the UKUSA Agreement (USA, United Kingdom, Australia, New Zealand and Canada) and designed to intercept communications on a worldwide basis was largely ruled out'. Although the existence of closer cooperation among the English-speaking countries was not in doubt, the committee had failed to find evidence that the cooperation was geared to the establishment of an integrated interception system or even a worldwide interception network. The committee felt it was likely that the name ECHELON denoted a stage reached in the development of technology for the interception of satellite communications. The report made explicitly clear that the Italian secret service SISMI had ruled out the existence of an automatic system for the recognition of words used in conversations, so that the targeted interception of conversations containing given keywords was not feasible.

[137] Il ruolo dei servizi di informazione e sicurezza nel caso 'Echelon'.' Relazione del comitato parlamentare per i servizi di informazione e sicurezza e per il segreto di stato. Approvata nella seduta del 29 novembre 2000. Trasmessa alle Presidenze il 19 dicembre 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 UKUSA 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 United Kingdom.

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[138], 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 antennae. The author, Erich Schmidt-Eenboom[139] claims that a station is also operating in New Caledonia and is used by the German Federal Intelligence Service.

Theoretically, since it meets the geographical, technical and financial requirements, 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 (Federal Agency of Government Communications and Information, Federalnoye Agentstvo Pravitelstvennoy Svyazi), which is responsible for communications security and SIGINT, operates ground stations in Latvia, Vietnam and Cuba in cooperation with the Russian military intelligence service GRU.

On the basis of the relevant legal provisions, FAPSI's role is to collect political, economic, military and scientific and technological information with a view to fostering economic, military and scientific and technological development[140]. In addition, in 1997 the Director of FAPSI described its primary tasks as the interception of encrypted foreign communications and global interception[141].

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. With the aid of this station, Russia both gathers strategic intelligence and intercepts military and

[138] *Jean Guisnel*, L'espionnage n'est plus un secret, The Tocqueville Connection, 10.7.1998.
Vincent Jauvert, Espionnage, comment la France écoute le monde, Le Nouvel Observateur, 5.4.2001, No 1900, 14 et seq.
[139] *Erich Schmidt-Eenboom*, in: Streng Geheim, Museumsstiftung Post und Telekommunikationn, Heidelberg (1999), 180.
[140] Russian Federation Federal Law on Foreign Intelligence, adopted by the Duma on 8 December 1995, Sections 5 and 11
[141] Quoted in *Gordon Bennett*, Conflict Studies and Research Centre, The Federal Agency of Government communications and Information, August 2000, http://www.csrc.ac.uk/pdfs/c105.pdf

commercial communications.[142] In the Indian Ocean there are stations in Russia, about which no further information is available. A further station in Skundra in Latvia was closed in 1998[143]. 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.

[142] Quoted in *Gordon Bennett*, Conflict Studies and Research Centre, The Federal Agency of Government Communications and Information, August 2000, http://www.csrc.ac.uk(pdfs/c105.pdf
[143] Homepage of the Federation of American Scientists (FAS), http://www.fas.org

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[144]. 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[145]. 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[146]. 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[147] and Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector[148] do not apply to 'the processing of data[149]/activities[150]

[144] See Chapter 1, 1.3, above.
[145] See Chapter 2 above.
[146] See Chapter 5, 5.6. and 5.8.
[147] OJ L 281 1995, p. 31.
[148] OJ L 24 1998, p. 1.
[149] Art. 3(2), Directive 95/46.
[150] Art. 1(3), Directive 97/66.

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[151] 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 EC's 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[152]. This regulation is also applicable only in so far as the bodies are acting within the framework of the EC Treaty[153]. 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[154].

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 telecommunications for security or intelligence purposes[155], the issue of infringement of Article 6(2) TEU does not yet arise.

---

[151] COM(2000) 385 final, OJ C 365 E/223.

[152] Regulation (EC) No 45/2001, OJ L 8, p.1.

[153] 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.'

[154] 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.

[155] 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

7.3. The question of compatibility in the event of misuse of the system for the purposes of gathering competitive intelligence

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[156], 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 to gather competitive intelligence, 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 in principle 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 in the broad sense. On the other 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.

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.

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

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[157], 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 UKUSA 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'[158].

8.2. The protection of privacy under international agreements

Many agreements under international law specify respect for privacy as a fundamental right[159]. At world level, particular mention should be made of the International Covenant on Civil and Political Rights[160], 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 UKUSA states have complied with the decisions taken by the Human Rights Committee set up

[157] 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'.

[158] 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.

[159] 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; Part. 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.

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

pursuant to Article 41 of the Covenant to rule on breaches of the Covenant under international law. The Optional Protocol[161], 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[162]. 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.

The Charter has not yet been incorporated into the Treaty. It is binding, therefore, only on the three institutions which pledged to comply with it in the Formal Declaration adopted during the Nice European Council: the Council, the Commission and the European Parliament. As far as your rapporteur is aware, they are not involved in any secret service activities. Even when the Charter acquires full legal force through its incorporation into the Treaty, due account will have to be taken of its limited scope. Pursuant to Article 51, the Charter applies to 'the institutions and bodies of the Union … and to the Member State only when they are implementing Union law'. Accordingly, the Charter would at best take effect via the ban on state aid schemes which run counter to the principles of competition (see Chapter 7, 7.3.).

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.

[161] Optional Protocol to the International Covenant on Civil and Political Rights, adopted by the UN General Assembly on 16 December 1966.
[162] '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[163].

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'[164]. 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[165].

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 legal basis under national law[166]. The law must be generally accessible and its consequences must be foreseeable[167].

---

[163] 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 *Francis G. Jacobs, Robin C. A. White*, The European Convention on Human Rights, Clarendon Press (1996), pp. 21 et seq, *Jochen Abr. Frowein, Wolfgang Peukert*, European Convention on Human Rights, N.P. Engel Verlag (1996), Rz 4 et seq.

[164] See European Court of Human Rights, Klass et al, 6.9.1978, line 41.

[165] 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.

[166] Under the case law of the European Court of Human Rights (in particular Sunday Times, 26.4.1979, line 47 et

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[168]. 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[169]. 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[170].

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[171]. Invasions of privacy may not be restricted to the absolute minimum, but mere usefulness or desirability is not sufficient justification[172]. The view that the interception of all

---

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. For more details see *Wolfgang Wesseley*, Telecommunications Privacy – an unknown basic right?, ÖJZ 1999, pp. 491 et seq, 495.

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

[168] 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.

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

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

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

[172] European Court of Human Rights, Silver et al, 24.10.1983, line 97.

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[173]. 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[174] and have made no move to set up a supervisory system similar to the office of parliamentary Ombudsman pioneered by the Nordic states[175]. Your rapporteur therefore welcomes the efforts made by the French National Assembly Committee on National Defence to set up a monitoring committee[176], 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.

---

[173] European Court of Human Rights, Leander, 26.3.1987, line 60.

[174] 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.

[175] For details of the situation regarding the supervision of intelligence services in the Member States, see Chapter 9.

[176] Bill entitled 'Proposition de loi tendant à la création de délégations parlementaires pour le renseignement', and the related report by *Arthur Paecht*, Rapport fait au nom de la Commission de la défense nationale et des forces armées sur la proposition de loi (N° 1497) de M. Paul Quilès et plusieurs de ses collègues tendant à la création d'une délégation parlementaire pour les affaires de renseignement, enregistré à la Présidence de l'assemblée nationale le 23. novembre 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[177].

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[178]. 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, a US 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 parties Germany and the United

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

[178] 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.

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 a US intelligence service, since only in the first instance is legal redress available in the national

courts[179]. 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 US authorities have repeatedly tried to justify the interception of telecommunications by accusing the European authorities of corruption and taking bribes[180]. 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.

[179] 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.
[180] *James Woolsey* (former CIA Director), Why America Spies on its Allies, The Wall Street Journal Europe, 22 March 2000, 31, and Remarks at the Foreign Press Centre, transcript, 7 March 2000, http://cryptome.org/echelon-cia.htm.

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[181], 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)[182].

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[183] it 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

[181] See Chapter 7.
[182] 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 Chapter 8, 8.3.2. above.
[183] 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[184]. 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[185], in other Member States – in some cases subject to authorisation by an independent commission[186] - it is carried out on the basis of a ministerial order[187], possibly even without restriction in the case of some communication media[188]. 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

[184] For comprehensive details of the activities of foreign intelligence services, see Chapter 2.
[185] For example, in Austria and Belgium.
[186] 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..
[187] 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).
[188] 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 at national level 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[189]) 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)[190], 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, monitoring of intelligence services is the exception in the Member States.

In France[191], 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

[189] 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.
[190] Law on the supervision of federal intelligence activities (PKGrG) of 17 June 1999, BGBl I 1334 idgF.
[191] 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[192], 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)[193], 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[194], Denmark[195], Germany[196], Italy[197], the Netherlands[198] and Portugal[199], there is a

[192] See the Bill entitled 'Proposition de loi tendant á la création de délégations parlementaires pour le renseignement', and the related report by *Arthur Paecht*, Rapport fait au nom de la Commission de la défense nationale et des forces armées sur la proposition de loi (N° 1497) de M. Paul Quilès et plusieurs de ses collègues tendant à la création d'une délégation parlementaire pour les affaires de renseignement, enregistré à la Présidence de L'Assemblée nationale le 23 novembre 1999

[193] Intelligence Services Act 1994, Section 10.

[194] 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.

[195] Udvalget vedrørende efterretningstjenesterne, Lov om etablering af et udvalg om forsvarets og politiets efterretningsjenester, lov 378 af 6.7.88.

parliamentary monitoring committee responsible for scrutinising both the military and civilian intelligence service. In the United Kingdom[200] 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[201] 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[202] and Sweden[203] 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.

---

[196] Das parlamentarische Kontrollgremium (PKGr), Gesetz über die Kontrolle nacrhichtendienstlicher Tätigkeit des Bundes (PKGrG) vom 17 Juni 1999 BGB1 I 1334 idgF.

[197] 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.

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

[199] Conselho de Fiscalização dos Serviços de Informações (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.

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

[201] 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.

[202] 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.

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

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 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[204].

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 Chapter 10, 10.1.14).

[204] Information for firms provided with security protection, Federal Ministry of Economic Affairs, 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[205]. 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[206]. 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[207] and with managers of US 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.

[205] *Michael E. Porter*, Competitive Strategy, Simon & Schuster (1998).
[206] *Roman Hummelt*, Industrial espionage on the data highway, Hanser Verlag (1997).
[207] Details and names confidential.

As early as 1988, the Max Planck Institute estimated that the damage caused by industrial espionage in Germany amounted to at least DM 8 billion[208]. The chairman of the association of security consultants in Germany, Klaus-Dieter Matschke, 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[209], 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[210].

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[211], 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[212].

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.

---

[208] Impulse, 3/97, 13 et seq.
[209] *Louis J. Freeh*, Director FBI, Statement for the Record, Hearing on Economic Espionage, House Judiciary Committee, Subcommittee on Crime, Washington DC, 9.5.1996
[210] *Robert Lyle*, Radio Liberty/Radio Free Europe, 10.2.1999.
[211] Computerzeitung, 30.11.1995, 2.
[212] *Roman Hummelt*, Spionage auf dem Datenhighway, Hanser Verlag (1997), 49 et seq.

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.

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, 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, 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, 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, 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 more than before 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[213].

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 Chapter 10, 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.

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

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;

- 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 US 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	Duncan Campbell in STOA 1999, Part 2/5, with reference to Baltimore Sun, America's Fortress of Spies, by Scott Shane and Tom Bowman, 3 December 1995, and Washington Post, Recent US Coups in New Espionnage, by William Drozdiak
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, 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; (breach of patent rights)	„Aktenkrieger“, SZ, 29 March 2001
Enercon	US firm Kenetech Windpower	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 legal action against Enercon for breach of patent rights on the grounds that Enercon had obtained commercial secrets illegally, According to an NSA employee, detailed information concerning Enercon was passed on to Kenetech via ECHELON	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	1995	Negotiations on the import of Japanese luxury cars Information on the emissions standards of Japanese cars	COMINT, no detailed information	Obtaining information	No details	Duncan Campbell in STOA, Part 2/5, 1999, with reference to Financial Post, Canada, 28 February 1998

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	Out of court settlement. In 1996, López resigns as VW manager, pays US$ 100 m to GM/Opel (supposedly lawyers' fees) and over a seven-year period purchases spare parts for a total of US$ 1 bn.	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	Duncan Campbell in STOA, 1999, Part 2/5, with reference to New York Times, How Washington Inc. Makes a Sale, by David Sanger, 19 February 1995, and 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.

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 US political system in particular this would give rise to a serious problem. US 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 economic matters in the post-Cold War era

Since 1990, the US Administration has increasingly come to equate national security with economic security. The annual White House report entitled 'National Security Strategy' repeatedly emphasises that **'economic security is fundamental not only to our national interests, but also to national security'**.

This development can be traced back to a number of sources. Essentially, three factors came together:

- the interest of the intelligence services in taking on a task which would outlive the Cold War;
- the US State Department's simple acknowledgement of the fact that, following the Cold War, the USA's leading role in the world could not be based solely on military strength, but also made economic strength essential;
- President Clinton's interest, from a domestic policy point of view, in strengthening the US economy and creating jobs.

This combination of interests had practical consequences.

As a logical response, since 1992, the FBI has focused its counterintelligence activities on industrial espionage and, in 1994, it set up an Economic Counterintelligence Program. Speaking to the US Congress, Louis J. Freeh, the Director of the FBI, described this as a **defensive** programme designed to prevent the competitiveness of the US economy from being undermined by the theft of information.

As a logical response, at least from an American point of view, the Administration has used the CIA, and subsequently the NSA, to prevent distortions of competition by means of bribery. The former Director of the CIA, James Woolsey, made this explicitly clear at a press conference he gave on 7 March 2000 at the request of the US State Department[214].

As a logical response, the US Department of Commerce has focused its efforts to foster exports in such a way that a US firm wishing to export goods need only deal with one agency. Active use is made of all the weapons at the Administration's disposal (for further details, see Chapter 10, 10.9.4).

[214] State Department Foreign Press Center briefing, Subject: Intelligence Gathering and Democracies: The Issue of Economic and Industrial Espionage, Washington DC, 7.3.2000

10.9.1. The challenge for the US Administration: industrial espionage against US firms

Intelligence operations directed against the US economy are neither unusual nor new. For decades, both the USA and other leading industrialised countries have been targets for industrial espionage. During the Cold War, however, economic and technological intelligence-gathering took second place to conventional espionage. Following the end of the Cold War, industrial espionage has come into its own[215].

In 1996, speaking to the US Congress, the Director of the FBI, Louis J. Freeh, gave a detailed account of the way the US economy has become a target for industrial espionage by other countries' intelligence agencies. As he put it, 'consequently foreign governments, through a variety of means, actively target US persons, firms, industries and the US Administration itself, to steal or wrongfully obtain critical technologies, data and information in order to provide their own industrial sectors with a competitive advantage'. However, the theft of information by Americans was increasing just as much. The further remarks made by Mr Freeh to the US Congress are summarised below. At this point, your rapporteur would like to express regret at the fact that the US Administration did not allow a delegation from the Temporary Committee to discuss these issues with the FBI. Up-to-date information could then have been obtained. In the paragraphs which follow, therefore, your rapporteur has assumed that the US Administration takes the view that the hearing before the House of Representatives held in 1996 gives an accurate picture of the threat currently posed to the US economy by industrial espionage. Accordingly, he has drawn extensively on that source.

10.9.1.1. The players

At the time of the hearing, the FBI was investigating persons or organisations from 23 countries who were suspected of industrial espionage against the USA. Some ideological or military opponents of the USA have merely continued their Cold War activities[216]. In contrast, other governments carry out industrial and technological espionage, even though they have long been the USA's military and political allies. In so doing, they often exploit their ease of access to US information. Some have developed agencies which assess information concerning high-technology products and use that information in competition with US firms. No countries have actually been named, although the involvement of Russia, Israel and France has been hinted at[217].

10.9.1.2. Objectives of industrial espionage

The objectives of industrial espionage named by the FBI in no way differ from those outlined in Chapter 10, 10.1.1. However, high-technology products and the defence industry are given as priority objectives. Interestingly enough, the FBI names information concerning bids, contracts, clients and strategic information in these areas as objectives of industrial espionage

[215] Statement for the Record of *Louis J. Freeh*, FBI Director, Hearing on Economic Espionage, House Judiciary Committee, Subcommittee on Crime, Washington DC, 9.5.1996
[216] 'The end of the Cold War has not resulted in a peace dividend regarding economic espionage', Statement for the Record of *Louis J. Freeh*, FBI Director, Hearing on Economic Espionage, House Judiciary Committee, Subcommittee on Crime, Washington DC, 9.5.1996
[217] Interpretation by your rapporteur of the cryptic remarks made by *Louis J. Freeh* to the committee.

which are pursued **aggressively**[218].

10.9.1.3. Methods

In the context of the **Economic Counterintelligence Program**, the FBI has identified a series of espionage methods. A combination of methods is employed in most cases, a single method only rarely. According to the information obtained by the FBI, the best source is a person employed by a firm or organisation, something which is not only true for the USA (see Chapter 10, 10.3. and 10.4.). At the hearing, the FBI outlined how persons are used to carry out for espionage, but astonishingly gave no details of electronic methods.

10.9.2. The attitude of the US Administration towards active industrial espionage

At a press conference[219], and in a conversation with members of the committee in Washington, the former Director of the CIA, James Woolsey, briefly summarised the interception activities of the US Secret Service 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. Questioned more closely, however, Woolsey gave no specific examples.

US firms are banned by law from payment 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. He categorically ruled out the possibility of espionage solely for the purposes of obtaining competitive intelligence.

At a hearing before the House Permanent Select Committee on Intelligence held on 12 April 2000, the current Director of the CIA, George J. Tenet, echoed Woolsey's comments: 'It is not the policy nor the practice of the United States to engage in espionage that would provide an unfair advantage to US companies'. At the same hearing, Tenet went on to say that information on the payment of bribes was forwarded to other government agencies so that they could help US firms[220]. In response to a supplementary question from Congressman Gibbons, Tenet admitted that there was no legal ban on the gathering of competitive

[218] In these areas the interception of communications is a promising method!

[219] *James Woolsey,* Remarks at the Foreign Press Center, Transcript, 7.3.2000, http://cryptome,org/echelon-cia.htm

[220] 'As I indicated also in my testimony, there are instances where we learn, that foreign companies or their governments bribe, lie, cheat or steal their way to disenfranchise American companies. When we generate this information, we take it to other appropriate agencies, make them aware of it. They use that information through other means and channels to see if they can assist an American company. But we play defence, we never play offense, and we never will play offense'.

intelligence; however, he saw no need for such a ban, given that the intelligence services were not involved in activities of that kind.

In the course of a conversation held with him in Washington, the chairman of the House Permanent Select Committee on Intelligence, Porter Goss, painted a similar picture of US interception activities.

10.9.3. Legal situation with regard to the payment of bribes to public officials[221]

The payment of bribes to secure contracts is a worldwide, and not simply European, phenomenon. According to the Bribe Payers Index (BPI) published by Transparency International in 1999, which ranks the 19 leading exporting countries on the basis of their willingness to offer bribes, Germany and the USA share ninth place. Sweden, Austria, The Netherlands, the United Kingdom and Belgium were identified as being less likely to offer bribes; only Spain, France and Italy have a higher rating[222].

The Americans refer to the corrupt practices employed by European firms to justify industrial espionage. This is questionable, not only because wrongdoings by individual firms cannot justify the comprehensive use of espionage. Such heavy-handed practices could only be tolerated if there were a legal vacuum in this area.

However, the legal measures taken to combat corruption are just as stringent in Europe as they are in the USA. In 1997, these shared interests led to the adoption of the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. The Convention requires the signatory states to make the payment of bribes to a foreign public official a criminal offence and contains, alongside a definition of the offence of bribery, provisions concerning penalties, jurisdiction and enforcement.

The Convention, which came into force on 15 February 1999, has been transposed and ratified by all the EU Member States except Ireland. The USA transposed the Convention by adopting the 1998 International Anti-Bribery and Fair Competition Act amending the Foreign Corrupt Practices Act (FCPA) of 1977, which imposes on firms a requirement to keep accounts and prohibits the payment of bribes to foreign public officials[223]. Neither in the USA nor in the EU Member States are bribes accepted as tax-deductible operating expenditure[224].

Whereas the OECD Convention is designed only to combat the payment of bribes to foreign public officials, in 1999 the Council of Europe adopted two more far-reaching agreements,

---

[221] *Albin Eser, Michael Überhofer, Barbara Huber* (Eds), Using the criminal law to combat corruption. A comparative survey of offences involving bribery, drawn up on behalf of the Bavarian Ministry of Justice, edition iuscrim (1997).

[222] The scale runs from 10 (low incidence of bribery) to 0 (high incidence of bribery): Sweden (8.3), Australia (8.1), Canada (8.1), Austria (7.8), Switzerland (7.7), Netherlands (7.4), United Kingdom (7.2), Belgium (6.8), Germany (6.2), USA (6.2), Singapore (5.7), Spain (5.3), France (5.2), Japan (5.1), Malaysia (3.9), Italy (3.7), Taiwan (3.5), South Korea (3.4) and China (3.1).
http://www.transparency.org/documents/cpi/index.html#bpi

[223] OFFICE OF THE CHIEF COUNSEL FOR INTERNATIONAL COMMERCE, Legal Aspects of International Trade and Investment, http://www.ita.doc.gov/legal/

[224] http://www.oecd.org/daf/nocorruption/annex3.htm

although neither has yet come into force. The Criminal Law Convention on Corruption[225] also encompasses bribery in the private sector. It was signed by all the EU Member States except Spain and by the USA, but as yet has been ratified only by Denmark.

The Civil Law Convention on Corruption[226] lays down rules governing liability and compensation, stipulating in particular that contracts and contract clauses which require firms to pay bribes will be deemed null and void. It has been signed by all the EU Member States except the Netherlands, Portugal and Spain; the USA has not signed.

The EU has adopted two further legal acts designed to combat bribery: the Convention on the fight against corruption involving officials and the Joint Action on corruption in the private sector.

The Convention on the fight against corruption involving officials of the European Communities or officials of the EU Member States[227] is designed to ensure that corruption and the payment of bribes to officials are criminal offences throughout the EU. The Member States undertake to make both the payment of bribes to an official and corruption criminal offences, regardless of whether one of their own officials, an official of another Member State or an EU official is involved.

The Joint Action on corruption in the private sector[228] is intended to ensure that corruption and the payment of bribes to firms are criminal offences. In that connection, criminal law penalties are laid down for both natural and legal persons. However, the scope of the Joint Action is more restricted than that of the Convention on the fight against bribery involving officials in that it requires the Member States only to punish actions carried out at least in part on their territory. Member States are free to extend this jurisdiction to cover actions carried out abroad by their own nationals or to the benefit of domestic legal persons. Germany and Austria have made instances of corruption carried out abroad criminal offences provided that they are also punishable in the country concerned.

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

By means of Executive Order 12870, in 1993 President Clinton set up the Trade Promotion Coordinating Committee (TPCC)[229]. Its role is to coordinate and develop a strategy for the US Administration's trade promotion policy. In accordance with the Executive Order, a representative of the National Security Council (NSC) also sits on the TPCC[230]. The NSC formulates the United States' national security policy with reference to domestic policy, foreign policy, military and intelligence issues. Each president alters the focus of the NSC's

[225] Criminal Law Convention on Corruption http://conventions.coe.int/treaty/EN/WhatYouWant.asp?NT=173&CM=8&DF=21/06/01

[226] Civil Law Convention on Corruption ETS no.: 174, http://conventions.coe.int/treaty/EN/WhatYouWant.asp?NT=174&CM=8&DF=21/06/01

[227] Convention, drawn up on the basis of Article K.3(2)(c) of the Treaty on European Union, on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union, OJ C 195, 25.6.1997, 2.

[228] Joint Action of 22 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, on corruption in the private sector (98/742/JHA), OJ L 358, 31.12.1998, 2.

[229] White House Archive, http://govinfo.library.unt.edu/npr/library/direct/orders/tradepromotion.html

[230] Homepage of the National Security Council (NSC), http://www.whitehouse.gov/nsc

work. On 21 January 1993, by means of PDD2, President Clinton expanded the NSC and, at the same time, placed more emphasis on economic issues in connection with the formulation of security policy. Members of the NSC include the President, the Vice-President, the Secretary of State and the Secretary of Defense. The Director of the CIA is an advisory member.

10.9.4.1. 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. It acts as the interface between the TPCC and the US economy. By its own account, since its inception in 1993 the Center has helped hundreds of US firms to win public contracts abroad.

The Advocacy Center helps US businesses by[231]:

- marshalling the resources of the US Administration - from the various financing, regulatory, country and sector experts, through the worldwide network of commercial officers, to the White House;
- fighting to level the playing field and promote open competition in the international bidding arena – from the multibillion dollar infrastructure project to the strategic contract for a small business;
- pursuing deals on behalf of US companies from start to finish, through 'hands-on' support;
- supporting US jobs and boosting US exports through the successes of US companies who successfully bid for overseas projects and contracts;
- assisting US firms with stalled negotiations due to foreign government inaction or 'red tape'.

10.9.4.2. The Advocacy's Center's operating methods[232]

Only the Director and a small staff complement of 12 persons work at the Center itself (situation as at 6 February 2001). The project managers cover the following areas: Russia and the newly independent countries; Africa, East Asia and the Pacific; the Middle East and North Africa; South Asia – Bangledesh, India, Pakistan, Sri Lanka; Europe and Turkey; China, Hong Kong and Taiwan; Canada, the Caribbean and Latin America; the aerospace, automobile and defence industries worldwide; and the telecommunications, IT and computer industries worldwide.

The Center 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, projects manufactured in the USA must make up at least 50% of the value of the goods delivered under any given contract.

10.9.4.3. Involvement of the CIA in the work of the TPCC

[231] TPCC brochure on the Advocacy Center, October 1996

[232] Homepage of the Advocacy Center, http://www.ita.doc.gov/td/advocacy/

Duncan Campbell submitted to the members of the Temporary Committee a number of declassified documents which provide evidence of CIA involvement in the work of the Advocacy Center. They include minutes of the Trade Promotion Coordinating Committee dealing with a meeting of the Indonesia Working Group held in July and August 1994[233]. According to the documents, a number of CIA staff members sit on the Working Group, whose task is to draw up a trade strategy for Indonesia. The CIA staff members are named in the minutes.
Moreover, the minutes show that one of the CIA staff members defines one objective of the Working Group as that of identifying main competitors and making this background information available to firms[234].

10.9.4.4. Open questions in connection with the Advocacy Center

The US Administration did not allow the discussion arranged between members of the Temporary Committee and representatives of the Center to take place. For that reason, much to your rapporteur's regret, two areas of doubt could not be cleared up:

a. the Temporary Committee has in its possession documents which provide evidence of CIA involvement in the work of the TPCC (see Chapter 10, 10.9.4.3.),

b. in its own information brochure (quoted above), the Advocacy Center acknowledges that it focuses the resources of 19 'US government agencies'. Elsewhere in the brochure, however, only 18 such agencies are listed, raising the issue of why the 19th cannot be named in public.

Your rapporteur can only assume that the discussion arranged with the Advocacy Center was cancelled because it is involved in activities which the US Administration wishes to keep secret.

10.10. Security of computer networks

10.10.1. The importance of this chapter

As already outlined in Chapter 10, 10.4., nowadays, alongside the use of spies, hacking into computer networks or the theft of data from laptop computers represents the second most effective method of industrial espionage. The information given in this chapter has no direct bearing on the existence or otherwise of a global system for the interception of international communications. However, in view of the Temporary Committee's aims, the chapter on industrial espionage must include brief details of one of its most powerful tools. This will certainly help readers to assess the significance of a system for the interception of international communications in connection with industrial espionage.

[233] TPCC Working Group Meeting, Agenda, 18.7.1994, TPCC Indonesia Advocacy-Finance Working Group, Distribution List, and Minutes of the meeting of 17.8.1994, from a letter from the US and Foreign Commercial Service of 25.8.1994.
[234] ibidem: 'Bob Beamer suggested that any primary competitors known to the group for these projects should be included as background information', Bob Beamer is one of the CIA representatives.

10.10.2. The risks inherent in the use by firms of modern information technology

Modern electronic data-processing technologies have been in common use by firms for some time now. Data of all kinds is stored in highly compressed form on a variety of media. Data stored on computer has now become one of the key aspects of commercial know-how. This transition from an industrial to an information society is opening up new opportunities, but, at the same time, creating substantial security risks[235].

10.10.2.1. The risks are increasing

The new risks which are emerging can be summarised as follows[236]:
More and more firms have computer networks and more and more information is being condensed in one place, with the result that it can be copied simply by hacking into the network. At the same time, other sensitive items of information are being decentralised and are thus not easily accessible in the context of a centralised security management strategy. The mobility of senior managers, who carry sensitive information with them on their laptop computers, is creating additional risks. The outsourcing of services is giving rise to new maintenance practices in the IT sphere as well which are highly questionable from a security point of view. A combination of the low status accorded to security staff in firms' management hierarchy and senior managers' ignorance of security issues is giving rise to misguided decisions.

10.10.2.2. Some of the risks in detail

Compression of information on compact media
Nowadays, firms' business secrets are stored in a physically very small area on compressed media. As a result, for example, the full plans for a new factory can be smuggled out of a firm on a substitute hard disk the size of a cigarette packet or copied electronically in minutes, without leaving any trace, by hacking into a computer network.

Decentralisation of secret information
In the era of large-scale computers, it was easy to monitor access to secret information, since only one computer was involved. Today, each employee connected to the network is provided with substantial computing capacity at his or her workstation. This is of course a great advantage for the staff member concerned, but a disaster from a security point of view.

Easier copying of information
In the era of hand-drawn plans and mechanical typewriters it was very difficult to copy large numbers of documents without being detected. Today, in the electronic era, it is easy. Large volumes of digitalised information can be copied easily, quickly and without leaving any trace. As a result, in many cases only one intervention is needed to obtain the material in question and the risk of being detected is correspondingly much lower.

Mobility of senior managers
Often without being properly aware of the fact, senior managers often carry strategically

---

[235] Computer espionage, Document 44, Federal Ministry for Economic Affairs, July 1998.
[236] *Roman Hummelt*, Industrial Espionage on the Data Highway, Hanser Verlag (1997).

important information about their firms with them on their laptop computers. The speed with which a copy of the hard disk can be made in the course of a 'customs check' or a search of a hotel room offers intelligence services substantial opportunities for action. Alternatively, the Notebook in question is simply stolen. Moreover, in view of the decentralisation involved it is difficult to incorporate into a central security management strategy the information stored on the hard disks of laptop computers used by a firm's senior managers.

Outsourcing of maintenance services
Although outsourcing may serve to reduce a firm's costs, in the sphere of information technology and the maintenance of telephone networks it allows technicians from outside the firm virtually unrestricted access to information. The associated risks cannot be over-emphasised.

Inadequate network administration
Alongside security loopholes in the software itself, which hackers repeatedly find, the most serious danger stems from network administrators who are not properly aware of the risks. In its basic form, Windows NT is configurated in such a way that it reveals almost all the information required for a successful attack on the network[237]. If these configurations and standard passwords are not changed, accessing the network is child's play. Firms often make the mistake of investing considerable amounts of time and money in the security of the firewall, but fail to protect the network properly against attacks from within[238].

10.10.3. Frequency of attacks on networks

The number of instances of computer networks being hacked into via the Internet is increasing every year[239]. In 1989, the Computer Emergency Response Team (CERT), an organisation set up in the USA in 1988 with the aim of improving Internet security, received notification of 132 security problems. In 1994, the figure had already risen to 2 241 and in 1996 it reached 2 573. The real figure is certainly much higher. This assumption was backed up by a large-scale simulation which the US Department of Defense carried out using its own computers. Systematic efforts were made to hack into 8 932 servers and mainframe computers from outside. In 7 860 cases these attempts proved successful, only 390 attempts were detected and no more than 19 cases were reported. A distinction must be drawn between attacks and security problems. An attack is a single attempt to gain unauthorised access to a system. A security problem consists of a number of related attacks. Extrapolating from their own long-term studies, the Pentagon and US universities have posited a figure of 20 000 security problems and 2 million attacks on the Internet annually.

10.10.4. Perpetrators and methods

The aim of foreign intelligence services which attack IT systems is to secure the information they contain, if at all possible without being detected. In principle, a distinction can be drawn between three groups of perpetrators with three different modi operandi.

In-house attackers with comprehensive access authorisation

[237] *George Kurtz, Stuart McClure, Joel Scambray,* Hacking exposed, Osborne/McGraw-Hill (2000), 94.
[238] *Martin Kuppinger,* Internet and Internet Security, Microsoft Press Deutschland (1998), 60.
[239] *Othmar Kyas,* Security on the Internet, International Thomson Publishing (1998), 23.

A spy who has been smuggled into a firm or whose services have been bought and who has risen to become a systems administrator or security administrator in a computer centre need only make extensive use of the powers officially granted to him in order to steal virtually all his employer's know-how. The same applies to a senior development engineer with unrestricted access authorisation to all a firm's databanks.

A spy of this kind offers maximum espionage effectiveness. However, if suspicions arise, the risk of detection is high, since the investigations immediately focus on the small group of persons who have comprehensive access to information. Moreover, it is pure coincidence if a spy secures comprehensive access authorisation.

In-house attackers with workstation access authorisation
A spy working within a firm has a clear advantage over a hacker attacking from the outside: he must overcome only the network security precautions, but no firewall. From an individual workstation, and provided that the person concerned has the requisite knowledge, the architecture of the network can be established and substantial volumes of information can be obtained, using the same techniques employed by an outside hacker and other techniques available only to persons working from within[240]. In addition, the spy can converse with colleagues without raising suspicion and obtain passwords by means of 'social engineering'.

The effectiveness of such a spy can be high, but is not as predictable as in the first case. The risk of detection is lower, particularly in the case of networks whose administrator pays little attention to the dangers of an attack from within. It is much easier to smuggle in a spy trained to hack into computer networks (trainees, guest researchers, etc.).

10.10.5. Attacks from outside by hackers

That hackers repeatedly gain unauthorised access to computer networks is well-known and well-documented. Intelligence services themselves now train specialists in the skills needed to hack into computer networks. The effectiveness of such an attack cannot be predicted or planned; it depends to a great extent on the effectiveness of the network defence mechanisms and on whether, for example, the network used by the research department is physically linked to the Internet. The level of risk involved for a professional spy is virtually zero; even if the attack is detected, the spy is somewhere else entirely.

10.11. Under-estimation of the risks

10.11.1. Risk-awareness in firms

As things stand, awareness of the risk of industrial espionage is not very well developed in individual firms. This is partly reflected in the fact that security officers often have middle-management rank and are not board members. However, security costs money and board members generally take an interest in security issues only when it is too late.

Large firms do at least have their own security departments and employ security specialists in the IT sphere as well. In contrast, small and medium-sized firms vary rarely employ security

[240] *Anonymous,* Hacker's guide, Markt & Technik-Verlag (1999).

experts and are generally happy enough if their data-processing equipment works properly. However, such firms as well may be targets for industrial espionage, since many of them are highly innovative. Moreover, in view of their integration in the production process medium-sized component suppliers offer a suitable basis for industrial espionage operations against large firms.

10.11.2. Risk-awareness among scientists

As a rule, researchers are interested only in their area of expertise and can therefore sometimes be an easy target for intelligence services. Your rapporteur has noted with some amazement that research institutes whose work has obvious practical applications communicate with each other using unencrypted e-mails and the science network. This is quite simply reckless.

10.11.3. Risk-awareness in the European institutions

10.11.3.1. European Central Bank

Information concerning preparations for decisions by the European Central Bank (ECB) could be of great value to intelligence services – and, it goes without saying, of course to the markets. At a meeting held in camera, the committee heard statements by representatives of the ECB concerning the security precautions taken to protect information. On that basis, your rapporteur has come to the conclusion that the ECB is aware of the risks and, as far as is feasible, is taking appropriate security measures. However, he has been supplied with information[241] suggesting that risk-awareness is low in certain national central banks.

10.11.3.2. Council of the European Union

Prior to the appointment of the High Representative for the common foreign and security policy, the Council focused its efforts in the area of secrecy on measures to keep information concerning decision-making procedures and the stances adopted by the Member State governments from the public and the European Parliament. It would have had no defence against a professional intelligence operation[242]. For example, technical maintenance in the interpreting booths was apparently carried out by an Israeli firm. The Council has now adopted security regulations[243] consistent with the standard within NATO.

10.11.3.3. European Parliament

Up to now, the European Parliament has never dealt with classified documents and therefore has no experience in the area of the protection of secrecy and no security culture. The need for such a culture will only arise if Parliament gains access to classified documents in the future. Otherwise, a general policy of secrecy is anathema for a parliament whose actions must be as transparent as possible. However, with a view to protecting informants and petitioners, provision should be made for the encryption of e-mails transmitted from one Member's office to another. At present, this is not possible.

10.11.3.4. European Commission

The European Commission has directorates-general which, by virtue of the information they deal with, have no need for secrecy rules or protection arrangements. Indeed, the reverse is

[241] Private information, source protected.
[242] Information supplied by members of COREPER and Council officials; sources protected.
[243] Council Decision of 19 March 2001 adopting the Council's security regulations, OJ L 101, 11.4.2001, 1.

true: complete transparency should be the norm in all areas which have a bearing on legislation. The European Parliament must employ a vigilant approach in order to ensure that, in these areas, the influence exerted on legislative proposals by interested firms, etc. is not masked even more than it already is through the unnecessary introduction of inappropriate secrecy rules.

Admittedly, there are areas of the Commission's work which involve the processing of sensitive information. Alongside Euratom, the most obvious areas are foreign relations, foreign trade and competition. On the basis of the information supplied by the directorates-general concerned to the committee at a meeting held in camera, and above all on the basis of other information available to your rapporteur, it is very doubtful as to whether the European Commission is properly aware of the risk of espionage and whether it takes a professional approach to the issue of security. Naturally enough, a public report is no place in which to outline security shortcomings. Nevertheless, your rapporteur sees a pressing need for the European Parliament to consider this issue in an appropriate manner.

However, it can be stated now that the encryption systems which the Commission employs when communicating with some of its external offices are outdated. This does not mean that the security standard is poor. However, the equipment currently in use is no longer manufactured and only roughly half of the external offices are equipped with encryption technology. The introduction of a new system working on the basis of encrypted e-mails is an urgent necessity.

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[244].

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

[244] 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)[245]. 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.

[245] *Otto 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, 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[246], 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.[247]

The drawback to this process is that it is not easy to generate large numbers of these random keys[248], 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[249], 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

---

[246] It was introduced by Major *Joseph Mauborgne*, head of the cryptographic research division of the American army; Simon Singh, The Code Book (1999), Carl Hanser Verlag 151.
[247] *Simon Singh*, The Code Book (1999), Carl Hanser Verlag 151 et seq.
[248] *Reinhard Wobst*, *Abenteuer Kryptologie*[2], Adison-Wesley (1998), 60.
[249] 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.

current or magnetic field ('light off'). ASCII[250] standardisation now prevails, whereby each letter is represented by a seven-figure combination of 0 and 1.[251] 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[252]. 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 US encryption standard[253]. 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[254] 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 US policy on cryptography.

---

[250] American Standard Code for Information Exchange.
[251] A= 1000001, B= 1000010, C=1000011, D=1000100, E= 1000101, etc.
[252] In binary terms, this number consists of 56 zeros and ones. See Singh, The Code Book, Carl Hanser Verlag (1999), 303.
[253] *Simon Singh*, The Code Book, Carl Hanser Verlag (1999), 302 et seq.
[254] It was created by two Belgian cryptographers working at the Catholic University of Louvain, *Joan Daemen* and *Vincent Rijmen*.

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

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[255]. 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[256]. 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[257]. Many people even claim that the problem is insoluble, but this theory has not yet been proved[258].

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.

---

[255] The idea of asymmetric encryption using the public-key process was devised by *Whitfield Diffie* and *Martin Hellmann.*
[256] *Simon Singh*, The Code Book, Carl Hanser Verlag (1999), 327.
[257] *Johannes Buchmann*, Factoring large integers, Spektrum der Wissenschaft 2, 1999, 6 et seq.
[258] *Simon Singh*, The Code Book, Carl Hanser Verlag (1999), 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 US firm NAI, but is still made available to private individuals free of charge[259]. 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 Economic Affairs 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[260].

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

[259] Information on the software can be found at www.pgpi.com.
[260] On quantum cryptology, see *Reinhard Wobst*, Abenteuer Kryptographie[2], Adison-Wesley (1998), 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 US 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[261]

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

[261] *Charles Grant,* Intimate relations. Can Britain play a leading role in European defence - and keep its special links to US intelligence? 4.2000, Centre for European Reform

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. Practical 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. Budgetary 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 the United Kingdom may be less interested in intra-European sharing, and because its EU partners may trust the United Kingdom less. Equally, if the US believes that the United Kingdom 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. 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. It may be assumed, in view of the evidence and the consistent pattern of statements from a very wide range of individuals and organisations, including American sources, that the system or parts of it were, at least for some time, code-named ECHELON. What is important is that its purpose is to intercept private and commercial communications, and not military communications.

Analysis has revealed that the technical capabilities of the system are probably not nearly as extensive as some sections of the media had assumed. Nevertheless, it is worrying that many senior Community figures, in particular European Commissioners, who gave evidence to the Temporary Committee, claimed to be unaware of this phenomenon.

The limits of the interception system

The surveillance system depends, in particular, upon worldwide interception of satellite communications. However, in areas characterised by a high volume of traffic 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 UKUSA 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 an even smaller proportion of those communications. However extensive the resources and capabilities for the interception of communications may be, the extremely high volume of traffic makes exhaustive, detailed monitoring of all communications impossible in practice.

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. France, thanks to its overseas territories, is the only EU Member State which is geographically and technically capable of operating a global interception system by itself. There is ample evidence that Russia also operates 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 misused 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.
At its meeting of 30 March 2000 the Council made clear that it cannot agree to the creation or existence of an interception system which does not comply with the rules laid down in the laws of the Member States and which breaches the fundamental principles designed to safeguard human dignity.

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 communications permanently and at random would be in violation of the principle of proportionality and would therefore 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 foreseeability, 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 and between the security authorities in the spheres of justice and home affairs, 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 US intelligence services do not merely gather general economic intelligence, but also intercept communications between firms, particularly where contracts are being awarded, and they justify this on the grounds of combating attempted bribery. Detailed interception poses the risk that information may be used as competitive intelligence, rather than combating corruption, even though the US and the United Kingdom state that they do not do so. However, the role of the Advocacy Center of the US Department of Commerce is still not totally clear and talks arranged with the Center with a view to clarifying the matter were cancelled. It should also be pointed out that an agreement on combating the bribery of officials, under which bribery is criminalised at international level, was adopted by the OECD in 1997, and this provides a further reason why individual cases of bribery cannot justify the interception of communications. At all events, it must be made clear that 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. Although it is frequently maintained that the global interception system considered in this report has been used in this way, 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, more and more frequently, 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, the development of telecommunications infrastructure, the creation of new transport systems, etc.) and it is necessary to consult the company's head office.
Risk and security awareness in small and medium-sized firms is unfortunately often inadequate and the dangers of economic espionage and the interception of communications are often not recognised.
Since security awareness is likewise not always well developed in the European institutions (with the exception of the European Central Bank, the Council Directorate-General for External Relations and the Commission Directorate-General for External Relations), immediate action is therefore necessary.

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

In December 1999 in Helsinki the European Council decided to develop more effective European military capabilities with a view to undertaking the full range of Petersberg tasks in support of the CFSP. In order to achieve this goal, by the year 2003 the Union was to be able to rapidly deploy units of about 50 000 – 60 000 troops which should be self-sustaining, including the necessary command, strategic reconnaissance and intelligence capabilities. The first steps towards such an autonomous intelligence capability have already been taken in the framework of the WEU and the standing Political and Security Committee. Cooperation among intelligence services within the EU seems essential 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. The European Parliament is in the process of implementing the Regulation (EC) No 1049/2001 on public access to European Parliament, Council and Commission documents by revising the provisions of its Rules of Procedure as regards access to sensitive documents.

13.2. 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 a proposal to protect private life, as guaranteed in Article 8 of the ECHR, 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 of the European Union are called upon to establish a European platform consisting of representatives of the national bodies that are responsible for monitoring Member States' performance in complying with fundamental and citizens' rights in order to scrutinise the consistency of national laws on the intelligence services with the ECHR and the EU Charter of Fundamental Rights, to review the legal provisions guaranteeing postal and communications secrecy, and, in addition, to reach agreement on a recommendation to the Member States on a Code of Conduct to be drawn up which guarantees 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 Member States are called upon, at the next Intergovernmental Conference, to adopt the EU Charter of Fundamental Rights as a legally binding and enforceable act in order to raise the standard of protection for fundamental rights, particularly with regard to the protection of privacy. The EU institutions are called upon to comply with the fundamental rights laid down in the Charter in their respective areas of responsibility and activity.

5. The European Union and the USA are called upon to conclude an agreement on the basis of which each party applies to the other the rules governing the protection of privacy and the confidentiality of business communications which are valid for its own citizens and firms.

6. The Member States are called upon to conclude an agreement with third countries aimed at providing increased protection of privacy for EU citizens, under which all contracting states give a commitment, where one contracting state intercepts communications in another contracting state, to inform the latter of the planned actions.

7. 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.

8. 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. The relevant US NGOs, in particular the ACLU (American Civil Liberties Union) and the EPIC (Electronic Privacy Information Center), are called upon to exert pressure on the US Administration to that end.

9. The Council and the Member States are strongly urged to establish as a matter of priority a system for the democratic monitoring and control of the autonomous European intelligence capability and other joint and coordinated intelligence activities at European level. The European Parliament should play an important role in this monitoring and control system.

National legislative measures to protect citizens and firms

10. The Member States are strongly urged to review their own legislation on the operations of the intelligence services to ensure that it is consistent with the fundamental rights laid down in the ECHR and in the case law of the European Court of Human Rights and, if necessary, to adopt appropriate legal provisions. They are called upon to afford all European citizens the same legal guarantees concerning the protection of privacy and the confidentiality of correspondence. Any of their laws which are discriminatory in terms of the surveillance powers granted to the secret services must be repealed.

11. The Member States are called upon to aspire to a common level of protection against intelligence operations and, to that end, to draw up a code of conduct 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. A similar code of conduct should be negotiated with the USA.

12. The Member States are called upon to pool their communications interception resources with a view to enhancing the effectiveness of the CFSP in the areas of intelligence-gathering and the fight against terrorism, nuclear proliferation or international drug trafficking, in accordance with the provisions governing the protection of citizens' privacy and the confidentiality of business communications, and subject to monitoring by the European Parliament, the Council and the Commission.

Specific legal measures to combat industrial espionage

13. The Member States are called upon to consider to what extent industrial espionage and the payment of bribes as a way 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. The USA, Canada, Australia and New Zealand are called upon to join this initiative.

14. The Member States are called upon to give a binding undertaking neither to engage in industrial espionage, either directly or behind the front offered by a foreign power active on their territory, nor to allow a foreign power to carry out such espionage from their territory, thereby acting in accordance with the letter and spirit of the EC Treaty.

15. The Member States and the US Administration are called upon to start an open US-EU dialogue on economic intelligence-gathering.

16. The authorities of the United Kingdom are called upon to explain their role in the UK/USA alliance in connection with the existence of a system of the 'ECHELON' type and its use for the purposes of industrial espionage.

17. The Member States are called upon to ensure that their intelligence services are not misused for the purposes of obtaining competitive intelligence, since this would be at odds with the Member States' duty of loyalty and the concept of a common market based on free competition.

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

18. The Member States are called upon to guarantee appropriate parliamentary and legal monitoring of their secret services. Those national parliaments which have no monitoring body responsible for scrutinising the activities of the intelligence services are called upon to set up such a body.

19. 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.

20. 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.

21. Germany and the United Kingdom 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

22. The Commission and Member States are called upon to inform their citizens and firms about the possibility of their international communications being intercepted. This information must be combined with practical assistance in developing and implementing comprehensive protection measures, not least as regards IT security.

23. The Commission, the Council and the Member States are called upon to develop and implement an effective and active policy for security in the information society. As part of that policy, specific attention should be given to increasing the awareness of all users

of modern communication systems of the need to protect confidential information. A Europe-wide, coordinated network of agencies capable of providing practical assistance in designing and implementing comprehensive protection strategies must be established.

24. 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.

25. 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. The Commission is called upon to lay down a standard for the level of security of e-mail software packages, placing those packages whose source code has not been made public in the 'least reliable' category.

26. 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.

Measures to improve security in the institutions

27. The Community institutions and the public administrations of the Member States are called upon to provide training for their staff and make their staff familiar with new encryption technologies and techniques by means of the necessary practical training and courses.

28. The Commission is instructed to have a security analysis carried out which will show what needs to be protected, and to have a protection strategy drawn up.

29. The Commission is called upon to update its encryption system in line with the latest developments, given that modernisation is urgently needed, and calls on the budgetary authority (the Council together with Parliament) to provide the necessary funding.

30. The competent committee is requested to draw up an own-initiative report on security and the protection of secrecy in the European institutions.

31. The Commission is called upon to ensure that data is protected in its own IT systems and to step up the protection of secrecy in relation to documents not accessible to the public.

32. The Commission and the Member States are called upon to invest in new technologies in the field of decryption and encryption techniques as part of the Sixth Research Framework Programme.

Other measures

33. 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.

34. The Commission is called upon to put forward a proposal to establish, in close cooperation with industry and the Member States, a Europe-wide, coordinated network of advisory centres - in particular in those Member States where such centres do not yet exist - 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.

35. The Commission is called upon to pay particular attention to the position of the applicant countries; if their lack of technological independence prevents them from implementing the requisite protective measures they should be given support.

36. 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.

EUROPEAN PARLIAMENT

1999 *2004*

Session document

FINAL
A5-0264/2001
Part 2

11 July 2001

REPORT

on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098 (INI))

Part 2: Minority Opinions
Annexes

Temporary Committee on the ECHELON Interception System

Rapporteur: Gerhard Schmid

EN

CONTENTS

Page

MINORITY OPINION by Giuseppe Di Lello, Pernille Frahm and Alain Krivine 4
MINORITY OPINION by Patricia McKenna and Ilka Schröder 5
MINORITY OPINION by Jean-Charles Marchiani 6
MINORITY OPINION by Maurizio Turco 7
Annex I: List of the experts who provided the committee with information 8
Annex II: Bibliography ..... 11 Annex III: Do
communications for the purpose of criminal prosecution 17

1. Preliminary remarks 17

2. Distinction between the interception of communications for the purpose of criminal prosecution and for the purpose of intelligence gathering 17

3. Activities in the EU in the field of interception of communications for the purpose of criminal prosecution 18

3.1. General remarks 18

3.2. Restriction of EU powers and responsibilities to technical arrangements 18

3.3. Activities and legal acts in the field of interception of telecommunications 19

4. Definitions and explanations concerning further international activities in the field of interception of telecommunications 21

Annex IV: 23

MINORITY OPINION by Giuseppe Di Lello, Pernille Frahm and Alain Krivine

The report by the Temporary Committee confirms the existence of the Echelon interception system which is administered by various countries, including the United Kingdom, a Member State of the European Union, with the cooperation of Germany.

An interception system of this nature, which does not differentiate between communications, data and documents, infringes the fundamental right to privacy guaranteed by Article 8 of the European Convention on Human Rights and Article 6 of the Treaty on European Union.

The system therefore flagrantly infringes the freedoms enjoyed by European citizens, the logic of the free market and the security of the Union. Whatever our support for or opposition to that logic and those treaties may be, such infringements are unacceptable.

In its conclusions, the report ought to have called on the United Kingdom to dissociate itself from the Echelon system and on Germany to close the listening post located on its soil. It is a matter of regret that the European Union is more preoccupied with industrial espionage than with individual monitoring.

MINORITY OPINION by Patricia McKenna and Ilka Schröder

This report makes an important point in emphasising that Echelon does exist, but it stops short of drawing political conclusions. It is hypocritical for the European Parliament to criticise the Echelon interception practice while taking part in plans to establish a European Secret Service.

No effective public control mechanism of secret services and their undemocratic practices exists globally. It is in the nature of secret services that they cannot be controlled. They must therefore be abolished. This report serves to legitimise a European Secret Service which will infringe fundamental rights - just as Echelon does.

For the majority in Parliament, the focus is industry, where profit interests are supposedly threatened by industrial espionage. However, the vital issue is that no one can communicate in confidence over distances any more. Political espionage is a much greater threat than economic espionage.

This report constantly plays down these dangers of Echelon, while it remains silent about plans to introduce the ENFOPOL interception system in the EU. Every society must take a fundamental decision whether or not to live under permanent control. By adopting this report, the European Parliament shows that it is not concerned about protecting human rights and citizens' liberties.

MINORITY OPINION by Jean-Charles Marchiani

The UEN Group was not surprised at the outcome of the vote on Mr Schmid's report which, originally, was supposed to concern itself with the Echelon espionage system set up by certain English-speaking countries.

From the outset, a majority within Parliament had clearly indicated its intentions, preferring to set up this temporary committee rather than a full-blown committee of inquiry. Accordingly, it had nothing else to fear from proceedings where the rapporteur's ability to create regular diversions was in no way threatened by a band of malcontents whose motives were too disparate.

Our message is crystal-clear: Mr Schmid's efforts have been unable to conceal either the existence of the Echelon system or the active or passive involvement of several Member States.

That has resulted in a serious breach of the principles underlying the treaties which ought to have led to sanctions being imposed or, at the very least, to measures being taken which might prevent intra-European solidarity from being subordinated to the imperatives of the solidarity of the English-speaking world.

Mr Schmid's weighty report is rich in information but does not properly address the central issue.
We therefore wish to distance ourselves from it and to reject a procedure which enables this Parliament, on the one hand, to take 'preventive' sanctions against a democratically elected government and, on the other, to refrain from so doing in instances such as this one.

MINORITY OPINION by Maurizio Turco

A. Although the likely existence of an Anglo-American system for the systematic and generalised interception of communications using search engines has been demonstrated, no reference is made to the fact that this technological capacity is certainly being used by Germany and the Netherlands and, probably, by France as well. Accordingly, since the secret services are intercepting communications from abroad, without authorisation and on the grounds of national security, some Member States will be intercepting communications from institutions, citizens or businesses of other Member States.

B. Although more powerful encryption methods should help to protect privacy, their introduction will inevitably lead to the appearance of more powerful lawful means of decryption techniques, given the indissoluble link between the development of cryptographic, code-breaking and technical interception systems.

C. Solutions must therefore be sought in the political field:
- via legal and parliamentary scrutiny of interception activities and monitoring of the police, security and intelligence services;
- by preventing the proliferation of control bodies which operate to different data-protection standards and without any genuine democratic and legal scrutiny,
- by regulating – on the basis of the highest standard and the case-law of the ECHR – protection of the privacy of European citizens against preventive interference by government authorities and eliminating the discrimination existing within the European Union between citizens of various Member States.

Annex I: List of the experts who provided the committee with information

1. Members of national parliaments

Mr Arthur PAECHT, French National Assembly
Mr Armand De DECKER, President of the Belgian Senate
Mrs Anne-Marie LIZIN, Belgian Senate
Mr Hans VAN HEVELE, Secretariat of the Belgian Senate
Mr Guilherme SILVA, Portuguese Parliament
Mr Ludwig STIEGLER, Bundestag (Lower House), Germany
Mr Dieter ANTONI, Austrian Parliament
Mr Desmond O´MALLEY, Irish Parliament

2. Representatives of the secret services

Mr Ernst UHRLAU, Secret Services Coordinator in the Federal Chancellery, Germany
Mr Harald WOLL, Baden-Württemberg Office for the Protection of the Constitution, Germany

3. Telecommunications, network and computer security experts

Mr José Manuel MENDES ESTEVES SERRA VERA, Technical Director, Banco Espirito Santo, Portugal
Mr Clive FEATHER, Head of Software Development, Demon Internet Ltd., United Kingdom
Mr Jacques VINCENT-CARREFOUR, former Head of Department for Network Security, France Telecom
Mr Bruno PELLERO, Expert Consultant in the monitoring of telecommunications, Italy
Mr Erhard MÖLLER, Mr Lutz BERNSTEIN and Mr Bernd SCHINKEN, Higher Institute Aachen, Germany

4. Authors and journalists concentrating on the ECHELON System

Mr Duncan CAMPBELL, United Kingdom
Mr Bo ELKJAER, Denmark
Mr Kenan SEEBERG, Denmark
Mr James BAMFORD, Washington DC
Mr Nicky HAGER, New Zealand

5. Encryption experts

Mr Reinhard WOBST, Unix Software, Germany
Mr Bernd ROELLGEN, Ciphers GmbH, Germany
Mr Peter BAHR, Ciphers GmbH, Germany
Mr Johan KEMPENAERS, KBC Bank, Belgium
Mr Leo VERHOEVEN, KBC Bank, Belgium
Herr Bart PRENEEL, Professor of Cryptology, Catholic University of Louvain, Belgium
Mr Danny de TEMMERMAN, European Commission
Mr Desmond PERKINS, European Commission

6. Experts on industrial espionage and related issues

Mr Sorbas VON COESTER, Director of Salamandre (Consultancy), France
Mr Christian HARBULOT, School for Economic Warfare, France
Mr Thierry LA FRAGETTE, Circé, France
Mr Ralf NEMEYER, Articon-Integralis, Germany

7. Human rights and protection of privacy

Mr Dimitri YERNAULT, Free University, Brussels
Mr Simon DAVIES, Privacy International, United Kingdom
Mr Jérôme THOREL, Privacy International, France
Mr Yaman AKDENIZ, Cyber Rights and Cyber Liberties, Leeds, United Kingdom
Mr David NATAF and Mr Alexandre COSTE, Millet-Sala-Nataf (law practice), Paris
Mr Rüdiger DOSSOW, Council of Europe, Strasbourg

8. Representatives of European Institutions

European Commission
Commissioner Christopher PATTEN (External Relations)
Commissioner António VITORINO (Justice and Home Affairs)
Commissioner Erkki LIIKANEN (Enterprise and the Information Society)
Mr Lodewijk BRIET, Directorate-General for External Relations
Mr Jacques DE BAENST, Head of Protocol and Security
Mrs Françoise DE BAIL, Directorate-General for Trade
Mrs Susan BINNS, Directorate-General for the Internal Market

Council of the European Union
Mr Brian CROWE, Director-General, External Relations
Mr Roland GENSON, Permanent Representative of Luxembourg, with special responsibility for Justice and Home Affairs
Mr Hervé MASUREL, representing the French Council Presidency
Ambassador Gunnar LUND, representing the Swedish Council Presidency

European Central Bank
Mr Christoph BOERSCH, Mr Wolfgang SCHUSTER and Mr Dominique DUBOIS, European Central Bank

9. Interlocutors during missions

Visit by the Chairman and rapporteur to Paris on 18-19 January 2001
Mr Jean-Claude MALLET, Secretary-General of SGDN
Mr Bertrand DUMONT, Air Marshal, Deputy Secretary-General, SGDN
Mrs Claude-France ARNOULD, Director of International and Strategic Affairs, SGDN
Mr Henri SERRES, Director with special responsibility for information systems security, SGDN
Mr Stéphane VERCLYTTE, Legal and European Affairs Adviser, SGDN
Mr Philippe DULUC, Scientific and Technical Affairs Adviser, SGDN
Mr Gérard ARAUD, Director of Strategic Affairs, Foreign Ministry
Mr Olivier MOREAU, Director of Security, Foreign Ministry
Mr Eric PERRAUDAU, Adviser, Defence Ministry
Mr. Jean-Pierre MILLET, lawyer

Visit by the Chairman and rapporteur to London on 24-26 January 2001
Mr Tom KING, Chairman of the Intelligence and Security Committee, House of Commons
Mr Alistair CORBETT, Head of the Secretariat of the ISC, House of Commons
Mr Donald ANDERSON, Chairman of the Foreign Affairs Committee, House of Commons
Mr Bruce GEORGE, Chairman of the Defence Committee, House of Commons
Mr Jack STRAW, Secretary of State for the Home Department
Mr Michael GILLESPIE, Security Service Coordinator
Mr Charles GRANT, Director, Centre for European Reform
Mr Casper BOWDEN, Director of FIPR

Visit by the committee bureau, the coordinators and the rapporteur to Washington DC on 6-12 May 2001
HE Günter BURGHARDT, Head of the Commission Delegation in Washington DC
Mr James WOOLSEY, former Director CIA
Mr Jeffrey RICHELSON, Director, National Security Archive, George Washington University
Mr Marc ROTENBERG, Electronic Information Privacy Centre
Mr Wayne MADSEN, Electronic Information Privacy Centre
Mr David SOBEL, Electronic Information Privacy Centre
Mr Barry STEINHARDT, Associate Director, American Civil Liberties Union
Mr Porter J. GOSS, Chairman of the House Permanent Select Committee on Intelligence
Ms Nancy PELOSI, Vice-Chairman of the House Permanent Select Committee on Intelligence
Mr Robert DAVIS, Deputy Counsel for the Office of Intelligence Policy Review, US Department of Justice.

Annex II: Bibliography

Literature quoted

Advocacy Center, Homepage, http://www.ita.doc.gov/td/advocacy/

Andrew, Christopher, The growth of the Australian Intelligence Community and the Anglo-American Connection, 223-224 in *E. Hayden, H. Peake and S. Halpern* eds, In the Name of Inteligence. Essays in Honor of Walter Pforzheimer (Washington NIBC Press 1995), 95-109

Andrew, Christopher, The making of the Anglo-American SIGINT Alliance, in: *Hayden B. Peake, Halpern, Samuel*. (Eds.): In the Name of Intelligence. Essays in Honor of Walter Pforzheimer, NIBC Press (1995), 95 -109

Andronov, Major *A.*, Zarubezhnoye voyennoye obozreniye, Nr.12, 1993, 37-43

Anonymous, Hacker's guide, Markt &Technik-Verlag (1999)

Bamford, James, Body of Secrets. Anatomy of the Ultra-Secret National Security Agency. From the Cold War through the Dawn of a new Century, Doubleday Books (2001)

Bamford, James, The Puzzle Palace. Inside the National Security Agency, America's most secret intelligence organization, Penguin Books (1983)

Bennett, Gordon, Conflict Studies and Research Center, The Federal Agency of Government Communications and Information, August 2000, http://www.csrc.ac.uk/pdfs/c105.pdf

Berliner Zeitung, Abgehört, 22.1.1996

Bode, Britta, Heinacher, Peter, Sicherheit muß künftig zur Chefsache erklärt werdenn Handelsblatt, 29.8.1996

Brady, Martin, Director of the DSD, Letter dated 16.3.1999 an Ross Coulthart, Sunday Program Channel 9; http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp; http://sunday.ninemsn.com/01_cover_stories/article_335.asp

Bronskill, Jim, Canada a key snooper in huge spy network, Ottawa Citizen, 24.10.2000, http://www.ottawacitizen.com/national/990522/2630510.html

Buchmann, Johannes, Faktorisierung großer Zahlen, Spektrum der Wissenschaft 2, 1999

Bundesministerium für Wirtschaft und Technologie der Bundesrepublik Deutschland, Computerspionage, Dokumentation Nr. 44, Juli 1998

Bundesministerium für Wirtschaft und Technologie der Bundesrepublik Deutschland, Informationen für geheimschutzbetreute Unternehmen (1997)

Bundesverfassungsgericht der Bundesrepublik Deutschland, BVerfG-Urteil, 1 BvR 2226/94 vom 14.7.1999 (zu Art. 10 GG, Gesetz zu Artikel 10 Grundgesetz)

Campbell, Duncan, 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, Part 2/5, in: STOA (Ed), Development of surveillance technology and risk of abuse of economic information (October 1999), PE 168.184

Campbell, Duncan, Inside Echelon, Heise Online, 24.7.2000, http://www.heise.de/tp/deutsch/special/ech/6928/1.html

Comité permanent de contrôle des services de renseignement, Rapport d'énquête sur la manière dont les services belges de renseignement réagissent face à l'éventualité d'un système americain "echelon" d'interception des communications téléphoniques et fax en Belgique, http://www.droit.fundp.ac.be/textes/echelonfr.pdf

Commission on the Roles and Capabilities of the US Intelligence Community, Preparing for the 21st Century: An Appraisal of U.S. Intelligence, (1996) http://www.gpo.gov/int/report.html

Deutscher Bundestag, Sekretariat des PKGr, Die Parlamentarische Kontrolle der Nachrichtendienste in Deutschland (2000)

Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet (Neuseeland), "Securing our Nation's Safety", Dezember 2000, http://www.dpmc.govt.nz/dess/securingoursafety/index.html

Dodel, Hans, Satellitenkommunikation, Hüthig Verlag (1999),

Elkjaer, Bo & Seeberg, Kenan, Echelon was my baby, Ekstra Bladet, 17.1.1999

Eser, Albin, Überhofer Michael, Huber Barbara (Eds), Korruptionsbekämpfung durch Strafrecht. Ein rechtsvergleichendes Gutachten zu den Bestechungsdelikten im Auftrag des Bayerischen Staatsministeriums der Justiz, edition iuscrim (1997)

Federation of American Scientists (FAS), Homepage, http://www.fas.org/

Fink, Manfred, Lauschziel Wirtschaft - Abhörgefahren und -techniken, Vorbeugung und Abwehr, Richard Boorberg Verlag, Stuttgart (1996)

Förster, Andreas, Maulwürfe in Nadelstreifen, Henschel Verlag (1997)

Frattini, Franco, Il ruolo dei servizi di informazione e sicurezza nel caso 'Echelon'. Relazione del comitato parlamentare per i servizi di informatione e sicurezza e per il segreto di stato. Approvata nella seduta del 29 novembre 2000, Trasmessa alle Presidenze il 19 dicembre 2000.

Freeh, Louis J, Statement for the Record, Hearing on Economic Espionage, House Judiciary Committee, Subcommittee on Crime, Washington DC, 9.5.1996

Freyer, Ulrich, Nachrichten-Übertragungstechnik, Hanser Verlag (2000)

Frost, Mike in a TV interview on NBC's "60 Minutes" on 27.2.2000, http://cryptome.org/echelon-60min.htm

Frost, Mike in an interview on Australian TV‘s Channel 9 on 23.3.1999 http://www.geocities.com/CapitolHill/Senate/8789/sunday1.htm

Frowein, Jochen Abr., Peukert, Wolfgang, Europäische Menschenrechtskonvention[2], N. P. Engel Verlag (1996)

Grant, Charles, Intimate relations. Can Britain play a leading role in European defence - and keep its special links to US intelligence? 4.2000, Centre for European Reform

Guisnel, Jean, L'espionnage n'est plus un secret, The Tocqueville Connection, 10.7.1998

Hager, Nicky, Secret Power. New Zealands´s Role in the International Spy Network, Craig Potton Publishing (1996)

Hager, Nicky, Exposing the global surveillance system, http://www.ncoic.com/echelon1.htm

Hoffmann, Wolfgang, Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V. (ASW), Aktuelle Anmerkungen zur Sicherheitslage der deutschen Wirtschaft, April 2001

Hummelt, Roman, Wirtschaftsspionage auf dem Datenhighway, Strategische Risiken und Spionageabwehr, Hanser Verlag (1997)

Intelligence and Security Committee (UK), Annual Report 1999-2000

Jacobs, Francis G, White, Robin C.A., The European Convention on Human Rights[2], Clarendon Press (1996)

Jauvert, Vincent, Espionnage - comment la France écoute le monde, Le Nouvel Observateur, 5.4.2001, Nr. 1900, S. 14 ff.

Kreye, Andrian, Aktenkrieger, Süddeutsche Zeitung, 29.3.2001

Kuppinger, Martin, Internet- und Intranetsicherheit, Microsoft Press Deutschland (1998), 60

Kurtz, George, McClure, Stuart, Scambray, Joel, Hacking exposed, Osborne/McGraw-Hill (2000)

Kyas, Othmar, Sicherheit im Internet, International Thomson Publishing (1998), 23

Landesamt für Verfassungsschutz Baden Württemberg, Wirtschaftsspionage, Die gewerbliche Wirtschaft im Visier fremder Nachrichtendienste, 10/1998

Legal Standards for the Intelligence Community in Conducting Electronic Surveillance, Report to the US Congress in late February 2000, http://www.fas.org/irp/nsa/standards.html

Leiberich, Otto, Vom diplomatischen Code zur Falltürfunktion - Hundert Jahre Kryptographie in Deutschland, Spektrum der Wissenschaft, Juni 1999

Lyle Robert, Radio Liberty/Radio Free Europe, 10 February 1999

National Security Councils (NSC), Homepage, http://www.whitehouse.gov/nsc

Madsen, Wayne in a TV interview on NBC's "60 Minutes" vom 27.2.2000, http://cryptome.org/echelon-60min.htm

Paecht, Arthur, 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, N° 2623 Assemblée nationale, enregisté à la Présidence de l'Assemblée nationale le 11 octobre 2000.

Paecht, Arthur, Rapport fait au nom de la Commission de la défense nationale et des forces armées sur la proposition de loi (N° 1497) de M. Paul Quilès et plusieurs de ses collègues tendant à la création d'une délégation parlementaire pour les affaires de renseignement, enregistré à la Présidence de l'Assemblée nationale le 23 novembre 1999

Porter, Michael E., Competitive Strategy, Simon & Schuster (1998)

Richelson, Jeffrey T., Desperately seeking Signals, The Bulletin of the Atomic Scientists Vol. 56, No. 2/2000, pp. 47-51, http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html

Richelson, Jeffrey T., The U.S. Intelligence Community[4], Westview Press, 1999

Richelson, Jeffrey T., The National Security Agency Declassified, National Security Archive Electronic Briefing Book no. 24, George Washington University http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html

Richelson, Jeffrey T., Ball, Desmond, The Ties That Bind, Boston Unwin Hyman (1985)

Richter, Nicolas, Klettern für die Konkurrenz, Süddeutsche Zeitung, 13.9.2000

Rötzer, Florian, Die NSA geht wegen Echelon an die Öffentlichkeit, Heise Online, 26.02.2000, http://www.heise.de/bin/tp/issue/download.cgi?artikelnr=6633&rub_ordner=special

Schmidt-Eenboom, Erich, Streng Geheim, Museumsstiftung Post und Telekommunikation Heidelberg, (1999)

Schütze, Arno, Wirtschaftsspionage: Was macht eigentlich die Konkurrenz? P.M. Magazin, Die Moderne Welt des Wissens (1998)

Shane Scott, Bowman Tom, America's Fortress of Spies, Baltimore Sun, 3.12.1995

Simon Singh, Geheime Botschaften, Carl Hanser Verlag (1999)

Smith, Bradley F., The Ultra-Magic Deals and the Most Secret Special Relationship 1940-1946, Presidio (1993)

Sorti, Francesco, Dossier esclusivo. Caso Echelon. Parla Luigi Ramponi. Anche I politici sapevano, Il Mondo, 17.4.1998

State Department Foreign Press Center Briefing, Subject: Intelligence Gathering and Democracies: The Issue of Economic and Industrial Espionage, Washington DC, 7.3.2000

Süddeutsche Zeitung, Haftstrafe wegen Spionage für Russland, 30.5.2000

TPCC, Broschüre über das Advocacy Center, Oktober 1996

Thaller, Georg Erwin, Satelliten im Erdorbit. Nachrichten, Fernsehen und Telefonate aus dem Weltall, Franzis Verlag, München (1999)

White House Archives http://govinfo.library.unt.edu/npr/library/direct/orders/tradepromotion.html

Wessely, Wolfgang, Das Fernmeldgeheimnis - ein unbekannts Grundrecht?, ÖJZ 1999, 491 ff

Wirtschaftswoche "Antennen gedreht", Nr. 46/9, November 1999

Wirtschaftswoche "Nicht gerade zimperlich", Nr. 43/16, Oktober 1992

Wobst, Reinhard, Abenteuer Kryptologie, Adison-Wesley (1998)

Woolsey, James, Why America Spies on its Allies, The Wall Street Journal Europe, 22.3.2000

Woolsey, *James,* Remarks at the Foreign Press Center, Transscript, 7.3.2000, http://cryptome.org/echelon-cia.htm

Wright, Steve, An appraisal of technologies for political control, STOA interim study (1998) PE 166.499/INT.ST.

Yernault, Dimitri, "Echelon" et l'Europe. La protection de la vie privée face à l'espionnage des communications, Journal des tribunaux, Droit Européen 2000, p. 187 ff.

FOR FURTHER READING

Air Intelligence Agency (AIA), Homepage, http://www.aia.af.mil

America´s Military Community, Homepage, http://www.military.com

Barr, Bob, Barr moves to expose "Project ECHELON", 9.11.1999, http://www.house.gov/barr/p_110999.html

Bundesnachrichtendienst, Die Nachrichtendienste der Bundesrepublik Deutschland, 2000, http://www.bundesnachrichtendienst.de/diensteb.htm

Bundesamt für Verfassungsschutz, Spionage gefährdet die Sicherheit und die Interessen unseres Landes, 2001, http://www.verfassungsschutz.de/arbeitsfelder/spion/page.html

Campbell, Duncan, Somebody´s listening, They´ve got it taped, 12.8.1988, New Statesman, http://jya.com/echelon-dc.htm

Central Intelligence Agency (CIA), Homepage http://www.odci.gov/index.html

Commander Submarine Force, U.S. Atlantic Fleet - Surveillance and Intelligence, http://www.sublant.navy.mil/roles.htm#survintel

Collingwood, John, Carnivore Diagnostic Tool, 16.8.2000, FBI-Press-Room http://www.fbi.gov/

Ecole de Guerre Economique, Homepage, http://www.ege.eslsca.fr/

Federal Bureau of Investigation (FBI), Homepage, http://www.fbi.gov

Frankfurter Allgemeine Zeitung, Niederländische Wirtschaftsspionage, 19.4.2000

Frankfurter Allgemeine Zeitung, Wirtschaftsspionage, 3.2.2001

Freeh, J. Louis, International espionage, 28.2.1996, Address before the Senate, http://www.fbi.gov

General Dynamics, Seawolf Class, http://www.gdeb.com/programs/seawolf/

Göbel, Jürgen, Kommunikationstechnik, Grundlagen und Anwendungen, Hüthig (1999)

Goss, J. Porter, Additional views of chairman Porter J. Goss, 2000, http://www.aclu.org/echelonwatch/goss.htm

Gralla, Preston, So funktioniert das Internet: ein virtueller Streifzug durch das Internet, Markt und Technik (1999)

Hager, Nicky, Wie ich Echelon erforscht habe, 11.04.2000, http://www.heise.de/tp/deutsch/special/ech/6728/1.html

Hayden, Michael, Statement for the record of House Permanent Select Committee on Intelligence, 12.04.2000 http://www.nsa.gov/releases/DIR_HPSCI_12APR.HTML

Innenministerium Brandenburg, Abwehr von Wirtschaftsspionage, 1999

Kerr, M. Donald, Congressional Statement on Carnivore Diagnostic Tool, 6.9.2000, http://www.fbi.gov

Kerr, M. Donald, Congressional Statement on Internet and Data-Interception Capabilities Developed by the FBI, 24.7.2000, http://www.fbi.gov

Mass, Christian, Satelliten Signale anzapfen und auswerten, Satellitenspionage für Einsteiger, Franzis Verlag, Funkschau Telekom, Poing 1998

Mathiesen, Thomas, On Globalisation of Control: Towards an Integrated Surveillance System in Europe, Statewatch Publication, 11.1999

Matschke, Klaus Dieter, Geheimdienste im Auftrag des Wettbewerbs, 5.9.1998, Seku Media Verlag Ingelheim

National Security Agency (NSA), Homepage, http://www.nsa.gov/

Preneel, Bart, Relative Security of Cryptographic, 18.11.1998, Presentation to Conference on Problems of Global Security

Schönleber, Claus, Verschlüsselungsverfahren für PC-Daten, Franzis Verlag, Poing 1995

Secretary of State for the Home Department, Interception of communications in the UK, June 1999

Sénat et Chambre des représentants de Belgique, 14.2.2000, Rapport d´activités 1999 du Comité permanent de contrôle des services de renseignements et de sécurité

Tenet, George, Statement by Director of Central Intelligence before the House Permanent Select Committee on Intelligence, 12.4.2000, http://sun00781.dn.net/irp/congress/2000_hr/tenet.html

The United States Navy, Homepage, http://www.navy.mil

The US Army Intelligence and Security Command (INSCOM), Homepage http://www.vulcan.belvoir.army.mil

The White House, Defending America's Cyberspace, National Plan for Information Systems Protection, Version 1.0, 2000, The White House 2000

Ulfkotte, Udo, Marktplatz der Diebe, Wie die Wirtschaftsspionage deutsche Unternehmen ausplündert und ruiniert. Bertelsmann Verlag, München (1999)

V. Bülow, Andreas, Im Namen des Staates. CIA, BND und die kriminellen Machenschaften der Geheimdienste. Piper Verlag, München (1998)

Verfassungsschutz Brandenburg, Abwehr von Wirtschaftsspionage - eine Aufgabe des Verfassungsschutzes, 1999, http://www.brandenburg.de/land/mi/vschutz/wispion.htm

Wall, Stephen, Permanent Representative of the United Kingdom to the European Union, Letter to Commissioner Liikanen concerning GCHQ, 21.3.2000

Wojahn, Jörg, Die globalen High-Tech-Schnüffler, 1.9.2000, Der Standard

Annex III: Definitions and explanations concerning the interception of communications for the purpose of criminal prosecution

1. Preliminary remarks

During the discussion in committee about the reliability, impact and dangers of the interception systems used world-wide by various intelligence services, reference was repeatedly made to measures and activities within the EU which, while involving the interception of communications, fell under the heading of judicial cooperation in criminal matters.

In the first part of this report, your rapporteur has, therefore, made no reference to those measures, since the issue of the legitimacy of intercepting communications for the purposes of criminal prosecution must not be confused with the legitimacy of intercepting communications for the purposes of intelligence gathering. Although interference in the private sphere, justified on security grounds (in the broadest sense of the term), is involved in both instances, the working methods and objectives are so different from each other that rules which might appear reasonable and balanced in one field would not necessarily be so for the other. The pertinence and proportionality of criminal prosecution measures should, therefore, not be discussed against the background of a political appraisal of measures relating to intelligence gathering.

At this juncture, in order to eliminate any uncertainties, reference will be made to particular issues raised, and definitions will be given of specific terms. Initially, a distinction will be drawn in Section 2 below between interception of communications for the purpose of criminal prosecution and interception for the purpose of intelligence gathering. Subsequently, in Section 3, reference will be made, with due account being taken of its powers and responsibilities, to EU legal acts involving interception of communications for the purpose of criminal prosecution. Finally, in Section 4, an explanation will be given of other terms used repeatedly in the committee's discussions in the context of international activities in the field of interception of communications.

2. Distinction between the interception of communications for the purpose of criminal prosecution and for the purpose of intelligence gathering

Interception of communications by foreign intelligence services (for example, by what is known as the ECHELON system) does not seek to monitor individuals in their home country but to carry out a general interception of traffic in a foreign country or countries in order, principally, to secure information which is relevant to national security. It is carried out in secret and, in the long term, does not aim to enter the public domain. Using the argument that secrecy alone can guarantee security and that they do not involve their own nationals, the secret services are frequently allowed to operate in a grey area as far as the law is concerned, where the rules are opaque and scrutiny inadequate.

On the other hand, where adequate suspicion exists, interception of communications for the purpose of criminal prosecution aims at preventing an offence from being committed or at punishing offences already committed. The interception measures are determined by the authorities in their home country. Should interception measures be required in a foreign

country, they are taken by the authorities in that country, on the basis of letters rogatory. Since the abolition of the police state, because the measures involve nationals, very specific rules and efficient control mechanisms have been established which seek to achieve a balance of interests. Interception measures may, therefore, be determined solely with regard to a specific case and where there is adequate suspicion that an offence may be about to be, or may have been, committed. In many Member States, court authorisation is required. Although the interception is carried out in secret, it aims solely at securing evidence to be used in open court. Accordingly, it is in the authorities' own interests to ensure that such evidence is acquired lawfully.

3. Activities in the EU in the field of interception of communications for the purpose of criminal prosecution

3.1. General remarks

The insertion in the Treaty on European Union of a Title relating to the common foreign and security policy created an opportunity for intelligence services to cooperate at European level, an opportunity which, however, has not to date been seized.
Where rules have been laid down and work has been carried out in the field of interception of communications at EU level, they have involved solely the criminal prosecution side, i.e. cooperation on matters relating to Justice and Home Affairs.

3.2. Restriction of EU powers and responsibilities to technical arrangements

As things stand, rules governing the admissibility of interception measures fall exclusively within the remit of the Member States. In accordance with the principle of limited powers, the EU may act only where powers and responsibilities are entrusted to it on the basis of the treaties. However, no provision is made for any such powers and responsibilities in Title VI of the EU Treaty entitled ‘Provisions on police and judicial cooperation in criminal matters’. In the field of police cooperation, Article 30(1) of the TEU provides for common action solely with regard to operational aspects, i.e. those which concern the ways and means of carrying out police work. In the field of judicial cooperation in criminal matters, although Article 31(c) provides in general terms, within the ambit of common action, for ‘ensuring compatibility in rules applicable in the Member States’, that is authorised only in so far ‘as may be necessary to improve [such] cooperation’. In other words, it is geared to cooperation-specific rules. Furthermore, the ‘approximation of rules on criminal matters’ in the Member States’ pursuant to the final indent of Article 29 restricts itself to the establishment of minimum rules relating to the constituent elements of criminal acts (Article 31(e)). To sum up, we may say that a decision on the issue of the conditions under which interception of communications is admissible remains a matter exclusively for national law. Your rapporteur is not aware of any efforts being made by any Member State to make changes to this purely national competence.

Cooperation between the Member States on the basis of the treaties may therefore come into play only when the issue is debated of the implementation of interception measures taken in accordance with national law, i.e. at a lower level. In instances where, on the basis of national law, interception of telecommunications is authorised, the Member State involved should be

able to call on the other Member States for technical assistance. Whether the technical simplification sought, which would without doubt improve the efficiency of transfrontier interception of communications for the purpose of criminal prosecution, particularly in the field of organised crime, is held to be good or bad depends largely on the extent of confidence felt in the constitutional state involved. However, it should be emphasised once again that – even if transfrontier interception of communications is technically simplified by the introduction of technical uniformity, and even if abuse in individual cases cannot be prevented – the conditions for the admissibility of interception cannot be affected since they are governed exclusively by national law.

3.3. Activities and legal acts in the field of interception of telecommunications

Only two legal acts have been adopted in the field of interception of telecommunications: the Council Resolution of 17 January 1995 on the lawful interception of telecommunications, the substance of which should be extended to cover third countries by means of a corresponding Memorandum of Understanding and in respect of which, furthermore, a proposal for an update was planned (both were drawn up as ENFOPOL documents), and the agreement on judicial assistance in criminal matters.

Council Resolution of 17 January 1995 on the lawful interception of telecommunications[262]

The Council Resolution of 17 January 1995 on the lawful interception of telecommunications seems to go back to the cooperation between experts in the International Law Enforcement Telecommunications Seminar (ILETS) (see Section 4 below) and largely to comply with the IUR (international user requirements) drawn up thereat.
The aim of the resolution is to seek to ensure that the requisite technical conditions are created in all the Member States and that the authorities, in accordance with national authorisation procedures, may actually obtain access to data, thus being able to exercise the powers granted to them by national law at the technical level.
To that end, an annex includes a very detailed list of Member States' 'Requirements'. The Council 'notes' that the Requirements 'constitute an important summary of the needs of the competent authorities for the technical implementation of legally authorised interception in modern telecommunications systems.' Such requirements include, for example, the provision of call-associated data in real time and the ability of network operators to transmit the intercepted communications to the law enforcement monitoring facility. In the resolution, the Council considers that the Requirements should be 'taken into account in the definition and implementation of measures …' and calls on the Member States and the Ministers responsible 'to cooperate … with the aim of implementing the Requirements in relation to network operators and service providers.'
At this juncture, it should be emphasised that the form of legal act selected – a resolution – is not binding in nature and that it therefore creates no rights and obligations for the Member States. The controversy which surrounded the resolution and the documents appertaining thereto resulted not so much from its substance but rather from the circumstances in which it was drawn up, in particular from the lack of transparency.

[262] OJ C 329, 4.11.1996.

Memorandum of Understanding

In a subsequent Memorandum of Understanding[263], third countries were invited to transpose into their national law the technical Requirements set out in the resolution of 17 January 1995. In addition, the aim was for technical innovations and the resultant new Requirements to be notified to both the FBI and the Council Secretariat. That was done because intelligence technology is frequently manufactured by multinational undertakings. Accordingly, cooperation was essential with the interception authorities in third countries where production plants were located.
The Memorandum of Understanding was signed on 23 November 1995 by the Member States of the EU and Norway, but not by any other third countries. The USA, Australia and Canada simply informed the Council in writing that they would initiate the process for the transposition of the provisions into national law[264].
Unfortunately, that text has still not been published, a fact which has given rise to extensive speculation in the press.

Draft Council resolution on the lawful interception of telecommunications in relation to new technologies

As your rapporteur pointed out in his report dated 23 April 1999[265], the draft Council resolution on the lawful interception of telecommunications in relation to new technologies is an update of the 1995 resolution. The new resolution is designed to make it clear that the 1995 Council resolution, which will be supplemented by a few new Requirements, also applies to new communications technologies, such as satellite and Internet communications, and that the previously used technical terms are to be interpreted, mutatis mutandis, with regard to the new technologies (e.g. telephone number recognition in the Internet). The European Parliament approved the draft[266], but the Council has temporarily shelved the project.

Convention on Mutual Assistance in Criminal Matters[267]

The second legal act is the Convention on Mutual Assistance in Criminal Matters. Articles 17 et seq. thereof lay down the conditions in which mutual assistance in criminal matters is possible with regard to interception of telecommunications. Without going into the rules in detail, your rapporteur would point out that the Convention in no way curtails the rights of the

---

[263] No 10.037/95 ENFOPOL 112 (unpublished).
For the substance, see the written answer given by the Austrian Interior Minister, Karl Schlögel, dated 16 December 1998 to the Written Question tabled by Alexander Van der Bellen, MP; 4739/AB XX. GP.
[264] To quote the Austrian Interior Minister, Karl Schlögel, (see previous footnote). The President-in-Office of the Council, Michiel Patijn, said, somewhat opaquely, in his answer to Oral Question H-0330/97 by Jonas Sjöstadt at Question Time on 14 May 1997 that 'these Requirements' (he was referring to the Requirements set out in the Council Resolution of 17 January 1995) had also been signed by the United States, Canada, Australia and Norway.
[265] A4-0243/99.
[266] Legislative resolution embodying the opinion of the European Parliament adopted on 7 May 1999 (OJ C 279, 1.10.1999, p. 498).
[267] 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 C 197, 12.7.2000, p. 1, Articles 17 et seq.

person or persons whose communications are intercepted, since the Member State in which the person or persons whose communications are intercepted is located may at all times refuse assistance if such assistance is not permitted under its own national law.

4. Definitions and explanations concerning further international activities in the field of interception of telecommunications

It is not only the various EU legal acts but also the disparate working parties set up in the field of security policy which have caused confusion. Some of the terms are therefore clarified below.

ILETS (International Law Enforcement Telecommunications Seminar)

ILET Seminars were originally an FBI initiative. In 1993, the FBI invited criminal prosecution authorities and intelligence services from friendly countries to attend a seminar on telecommunications interception being held in Quanitco. Most of the current Member States of the EU, as well as Australia and Canada, attended the seminar[268]. Since then, regular meetings have been held in order to discuss requirements for efficient international communications interception.
At a meeting held in Bonn in 1994, the members of ILETS approved a document setting out policy guidelines, an annex to which included a list of international user requirements (IUR 1.0 or IUR 95). That list included the Requirements to be imposed on the various telecommunications operators in order to simplify the interception system. The IUR 1.0 served – albeit unofficially – as the basis for the Council Resolution of 17 January 1995 on the lawful interception of telecommunications. Subsequently, further meetings of experts were held to discuss IUR and their possible transposition and adjustment to cope with new telecommunications technologies.

TREVI Group

Meeting as the Trevi Group before the entry into force of the Treaty of Maastricht (which introduced provisions to govern cooperation in the fields of justice and home affairs in the Treaty on European Union), the Justice and Home Affairs Ministers discussed internal security issues. The Trevi Group is now defunct, since the topics involved are now dealt with in specific Council working parties.
With respect to the field at issue here, specific reference should be made to two such working parties, the Working Party on Mutual Assistance in Criminal Matters - which, as part of the activities for cooperation in justice and home affairs, dealt with the Convention on Mutual Assistance in Criminal Matters - and the Working Party on Police Cooperation, which was concerned with issues connected with the lawful interception of telecommunications traffic, including the monitoring of new communications systems (mobile telephones, Internet, e-mail). The latter was also involved in the approximation of the standards of the Requirements of the authorities competent to order interception of telecommunications imposed on network operators and service suppliers.

[268] For the substance of that seminar, see the written answer given by the Austrian Interior Minister, Karl Schlögel, to the Question tabled by Mr Van der Bellen, MP. 4014/AB XX.GP. http://www.parlinkom.gv.at/pd/pm/XX/AB/texte/AB04014_.html.

ENFOPOL

Despite the belief held by a number of writers, ENFOPOL is not a working party or an organisation, it is an abbreviation used for the designation of working papers in criminal prosecution and police matters drawn up, for example, by the Working Party on Police Cooperation[269]. The various documents are not given an ENFOPOL title, they are simply classified under that reference.

[269] See the oral answer given by Austrian Interior Minister, Karl Schlögel, to the Question tabled by Mr Van der Bellen, MP, 4739/AB XX.GP http://www.parlinkom.gv.at/pm/XX/AB/texte/040/AB04014_.html and Campbell, Duncan, ILETS, the secret hand behind ENFOPOL 98, http//heise.de/deutsch/special/enfo/6396/1.html.

ANNEX IV

SUMMARY

OF THE

INTELLIGENCE SERVICES AND PARLIAMENTARY CONTROL BODIES

OF THE

MEMBER STATES AND OF THE UKUSA STATES

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
AUSTRIA	***Heeresnachrichtenamt (HnA)*** ***Abwehramt (AbwA)*** military intelligence service reports to the Minister of Defence	*§ 20 Abs 3 Militärbefugnisgesetz (MBG) BGBl I 86/2000'*	military intelligence; counter-intelligence to combat threats to national security from abroad		parliamentary subcommittee: *Ständiger Unter-ausschuss des Landesverteidigungs-ausschusses zur Überprüfung von nachrichten-dienstlichen Maß-nahmen zur Siche-rung der militärischen Landesverteidigung (14 members; each party in Parliament must be represented)* *1 legal protection representative*	*A* *B* *ge* *§§* *G* *19*

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
AUSTRIA	**Sondereinheit für Observation (SEO)** civil intelligence service reports to the Minister of the Interior	*§§ 6, 14, 15 Sicherheitspolizei-gesetz (SPG, BGBl 566/1991 idgF);* *Sondereinheiten-Verordnung* (BGBl II 207/1998)	preserving public safety; internal counter-intelligence; protecting principles guaranteed by the Constitution; counteracting extremist movements, terrorism and organised crime		parliamentary subcommittee: *Ständiger Unter-ausschuss des Ausschusses für innere Angelegen-heiten zur Über-prüfung von Maß-nahmen zum Schutz der verfassungs-mäßigen Einrichtungen und ihrer Handlungs-fähigkeit (14 members; each party in Parliament must be represented)* *1 legal protection representative*	

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
BELGIUM	**Service Général du Renseignement et de la Sécurité des Forces armées(SGR)** **military intelligence and security service** reports to the Minister of Defence	*Loi du 30 novembre 1998 organique des services de renseignement et de sécurité*	obtaining information and data in the military, political, economic and technological/scientific field, responsible for the security of military installations and personnel		*Comité permanent de contrôle des services de renseignements et de sécurité (Comité permanent R),* three members appointed by the Senate; they may not hold electoral office or carry out any other activity that might jeopardise their independence *Service d'enquêtes des services de renseignements* attached to the Comité permanent R, members appointed by the Comité R	*Lo (V co de re*
BELGIUM	**Sûreté de l'Etat (VS)** **civil intelligence and security service** reports to the Minister of Justice	*Loi du 30 novembre 1998 organique des services de renseignement et de sécurité*	responsible for internal and external security, counter-intelligence, observation of political extremism			

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority
DENMARK	Forsvarets Efterretningstjeneste (FE(T)) **'Military Secret Service'** reports to the Minister of Defence	*Lov om forsvarets formål, opgaver og organisation m.v.* *Lov 909 af 8/12/1993* ['framework-law', in which FE(T) is not mentioned] [a new law on FET & PET will be adopted in the near future]	collecting and analysing secret information relevant to defence on the CIS, Central and Eastern Europe in the military, political, economic and technological/scientific fields, SIGINT; decryption staff & budget: classified information	yes	2 control committees: *Kontroludvalget vedrørende Politiets og Forsvarets efterretningstjenester (Wamberg-udvalget) (consisting of civil servants and lawyers)* appointed by the Minister of Justice *Udvalget vedrørende efterretningstjenesterne* parliamentary committee (consisting of 5 Members of the Danish Parliament)

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority
DENMARK	Politiets Efterretningstjeneste (PET) **'Police Secret Service'** reports to the Minister of Justice	no specific legislation [a new law on FET & PET will be adopted in the near future]	counter-intelligence, prevention of and action against activities which might endanger Denmark's security: espionage, terrorism, etc.; security of the Government and of the Royal Family staff: about 370 (1998) budget: classified information.		

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
FINLAND	**Pääesikunnan tiedusteluosasto 'Military Intelligence Division of the Finnish Defence Staff'** reports to the Minister of Defence	*Laki puolustusvoimista* N:o 402/1974 2§ 'Defence Forces Act' (Intelligence Division not mentioned)	surveillance of the country's land and sea areas and airspace in cooperation with other supervisory authorities, ensuring territorial integrity of the country	yes	no specific control body Ministry of Defence submits an annual report on interception to the Parliamentary Ombudsman	*P* *§3* 'P *La* *m* *40* 'O Ac [c Pa O re re M

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
FINLAND	**Suojelupoliisi (SUPO) 'Finnish Security Police'** reports to the Minister of the Interior	*Laki poliisin hallinnosta N:o 110/1992, 1§, 10§ 1. ja 2. momentti* *Asetus poliisin hallinnosta N:o 158/1996 8§* *Laki poliisin henkilörekistereistä N:o 509/1995 23§, 9§* 'Act and Decree on Police Administration', 'Police Personal Data' Act	counter-intelligence; averting activities which might endanger Finland's internal security and international relations, action against terrorism, preventive work for security		no specific control body; the police has to report all cases of interception to the Minister of the Interior, who submits an annual report to the Parliamentary Ombudsman	
FINLAND	**Tullin tiedusteluyksikkö 'Intelligence Section of the Finnish Customs'** reports to the Ministry of Finance	*Tullilaki N:o 1466/1994* 'Customs Act'	collecting and analysing data to prevent and uncover customs offences, and supplying such data to the relevant authorities for further action		no specific control body the customs have to report all cases of interception to the National Customs Board and to the Minister of the Interior, who submits an annual report to the Parliamentary Ombudsman	

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
FRANCE	**Direction générale de la sécurité extérieure (DGSE)** reports to the Ministry of Defence	*Décret n°82-306 du 2 avril 1982*	collecting intelligence data of political, economic and technological/scientific relevance, collecting and analysing intelligence of interest to the security of France, counter-espionage (outside national territory) 4100 Staff Budget: FF 1.7 billion	yes	no special parliamentary control body at the moment (under discussion; the Defence Committee of the National Assembly has twice proposed that a surveillance-type committee should be established; Nos 1951 and 2270) Commission nationale de contrôle des interceptions de sécurité' (exclusively scrutiny of interception of communications by means of wire-tapping) Members of this body include 1 MP and 1 Senator	

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
FRANCE	**Direction du renseignement militaire (DRM)** reports to the Ministry of Defence	*Décret n°92-523 du 16 juin 1992*	provides military intelligence necessary for the armed services 1700 staff, Budget FF 90 million, internal military security, supporting the army;			
FRANCE	**Direction de la surveillance du territoire (DST)** Civilian intelligence service reports to the Minister of the Interior	*Décret n°82-1100 du 22 décembre 1982*	Counter-espionage on French territory 1500 staff; protecting public safety, internal counter-intelligence			

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
GERMANY	**Bundesnachrichten-dienst (BND)** reports to the Federal Chancellor	*Gesetz über den Bundesnachrichten-dienst (BNDG),* BGBl 1990 I 2954 idgF	collecting and analysing intelligence on foreign activities of relevance to security and foreign policy	yes	*Parlamentarisches Kontrollgremium (PKGR*) parliamentary control body for all 3 secret services consists of 9 MPs (Members of the Bundestag)	*G* *Ko* *di* *de* *(F* *19* *id*
GERMANY	**Bundesamt für Verfassungsschutz (BfV)** reports to the Minister of the Interior	*Gesetz über die Zusammenarbeit des Bundes und der Länder in Angele-genheiten des Ver-fassungsschutzes und über das Bundsamt für den Verfassungs-schutz* (BVerfSchG, BGBl 1090 I 2954)	collecting and analysing intelligence on activities endangering security and activities of hostile intelligence services within Germany		*G 10-Kommission* not bound to take instructions; may, but need not, include MPs; 4 Members appointed by the PKGR	*§* *G* *G* *(G* *Au* *94* *(L* *Pa* *Te* *Se*
GERMANY	**Militärischer Abschirmdient (MAD)** reports to the Minister of Defence	*Gesetz über den militärischen Ab-schirmdienst (MADG*) BGBl 1990 I 2954 idgF	safeguarding the army's effectiveness protecting the security of military installations and military personnel			

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
GREECE	Ethniki Ypiresia Pliroforion (EYP) 'National Intelligence Service' reports to the KYSEA (National Security Council: Prime Minister + Ministers of Foreign Affairs and Defence)	Law 1645/86 on the National Intelligence Service *(Ethniki Ypiresia Pliroforion)*	* collecting and analysing information pertaining to the country's national security (information on organised crime, terrorism, military, economic and political information); forwarding of such information to the competent authorities * counter-intelligence; observation of activities of foreign intelligence services directed against the country.		Special parliamentary committee for the protection of communications and privacy. No specific control rights. Membership: 1 Vice-President of Parliament, 1 Member of each political group, 1 communications specialist	La *Ap* (S co
					Institution for the Protection of Personal Data	La *Pr* *ep* *de* *pr* (P Pe

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
IRELAND	**Garda Síochána** (national police service) deals with national security issues The police service reports to the Minister of Justice	Authority to intercept based on *Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993*	Interception authorised in the interests of the security of the State		*Joint Committee on Justice, Equality and Women's Rights* has responsibility for the general area of civil rights	
IRELAND	Intelligence Staff		national security interests of Ireland (mainly the IRA), security of national armed forces, technological developments of foreign armed forces		No special control authority	

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
ITALY	**Servizio per le informazioni e la sicurezza militare (SISMI)** **Servicio informazione operative Segrete (SIOS)** reports to the Minister of Defence who also appoints the Director of the Service and senior civil servants	*L. 24 ottobre 1977, n. 801, art. 4 Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato*	Military defence intelligence and security duties to protect the independence and integrity of the State, counter-espionage, collecting foreign intelligence on political, military, economic and technological/scientific subjects	yes	Parliamentary Committee (4 MPs + 4 Senators) The Government submits a six-monthly report to Parliament on information and security policy	L. 80 *Is* *or* *se* *in* *si* *de*
ITALY	**Servizio per le informazioni e la sicurezza democratica (SISDE)** **Direzione investigazioni anti-mafia (DIA)** reports to the Minister of the Interior who also appoints the Director of the Service and senior civil servants	*L. 24 ottobre 1977, n. 801, art. 6 Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato*	intelligence and security duties for the defence of the democratic State and its institutions intelligence on activities endangering internal security; counter-espionage to combat terrorism and organised crime			

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
LUXEM-BOURG	**Service de renseignement** national intelligence and security service reports to the Minister of State (= Prime Minister)	*Loi concernant la protection des secrets intéressant la sécurité extérieure de l'État du 30 juillet 1960*	protecting secrets under Article 120(vii) of the Criminal Code* and obtaining information necessary to safeguard the external security of the Grand Duchy and States with which it has concluded a regional joint defence agreement * 'offences against the GD of Luxembourg'		no parliamentary scrutiny (surveillance of any kind of communications to seek out offences against State security requires the assent of a committee comprising the chairman of the Supreme Court, the chairman of the Legal Affairs Committee of the Council of State and the chairman of the Chamber of Auditors)	*(L 19 in d' de 88*

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
NETHER-LANDS	**Militaire Inlichtingendienst (MID** or, more recently, MIVD) reports to the Ministry of Defence	*Wet op de inlichtingen- en veiligheidsdiensten* Law 635/87 of 3 December 1987, most recently amended by Law 194/1999 of 19 April 1999. [New bill under discussion]	military intelligence; intelligence-gathering on foreign armed forces	yes	*Tweede-Kamercommissie voor de Inlichtingen- en veiligheidsdiensten* 'Second Chamber Committee for Information and Security Services' parliamentary committee (4 members: the chairmen of the 4 major political parties)	*17 or Ka G* Ru Ne Cl '0 In Se
NETHER-LANDS	**Binnenlandse Veiligheidsdienst** (**BVD** or, more recently, AIVD) reports to the Ministry of the Interior		Internal security service, counteracting right- and left-wing extremism, counter-intelligence			

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
PORTUGAL	**Serviçio de Informações Estratégicas de Defesa e Militares (SIEDM)** reports to the Minister of Defence	Law 30/84 of 5 September 1984, amended by Law 4/95 of 21 February 1995, Law 15/96 of 30 April 1996 and Law 75-A/97 of 22 July 1997	foreign intelligence service; strategic intelligence service for political, military and economic affairs		*Conselho de Fiscalização dos Serviços de Informações (CFSI).* Consists of three citizens elected by the *Assembleia da República* (national parliament) for a period of four years. the *Assemblea da República* can call both Directors of SIS and SIEDM to be heard before a parliamentary committee	Th co do al
PORTUGAL	**Serviço de Informações de Seguranca (SIS)** reports to the Minister of the Interior		security service for internal affairs; protecting the Constitution (no executive powers); collecting and evaluating intelligence on criminal and anti-State activities			

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
SPAIN	**Centro Superior de Información de la Defensa (CESID)** reports to the Minister of Defence	*R.D. 2632/1985 de 27.12.1985 (BOE 20.01.1986) Estructura interna y relaciones del Centro Superior de la Defensa;* as amended by *R.D. 266/1996 de 16.02.1996 Modif. de la estructura organica del CESID*	foreign and internal intelligence service; procurement of political, economic, technological/scientific and military information; foreign intelligence coverage, counter-intelligence inside and outside Spain	yes	no specific control body; general parliamentary scrutiny by parliamentary committees as with other government authorities	
SPAIN	**Dirección General de la Guardia Civil (GC)** reports to the Minister of Defence and the Minister of the Interior	*L.Org. 2/1986 de 13.03.1986 (BOE 14.03.1986) de Fuerzas y cuerpos de seguridad*	Central Spanish paramilitary police authority including police intelligence service; fight against organised crime on Spanish territory			
SPAIN	**Dirección General de la Policia** reports to the Ministry of the Interior		Central Spanish police authority, including police intelligence service; internal and foreign intelligence relating to terrorist structures and Islamic fundamentalism in the Middle East and North Africa			

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
SWEDEN	Säkerhetspolisen (SÄPO) Civilian Intelligence and Security Service reports to the Minister of Justice	*Polislag (1984:387)* *Förordning (1989:773) med instruktion för Rikspolisstyrelsen* 'Police Act (1984:387) Ordinance (1989:773) and Directive for the National Police Board'	Responsibilities: - Security control - Counter-intelligence - Counter-terrorism - Protection of the Constitution Staff during 1999 about 800. 1995 Budget SEK 475 million (EUR 55.7 million)		Control body of the NPB, consisting of five MPs, two members of staff and the National Police Commissioner. *Registernämnd*, which consists of a maximum of eight members. At the moment there are two law officers, two MPs, a lawyer and an expert. Both bodies report to the Government	*Fo* *m* *R* 'C ar Na *Fo* *m* *R* 'C ar Re

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
SWEDEN	**Militära Underrättelse och Säkerhetstjänsten (MUST)** 'Military intelligence and security directorate'; Part of the Swedish military headquarters. military intelligence and security service reports to Minister of Defence	*Act 2000:130 and Ordinance 2000:131 on military intelligence service*	collection and analysis of secret military or political intelligence; counter-intelligence; counteracting subversion, sabotage and disorder; protecting the armed forces and arms industry		*Försvarets underrättelsenämnd* 'Defence Intelligence Control Commission', consists in part of MPs	*O w F u M C*
SWEDEN	**Försvarets Radioanstalt (FRA)** **independent special unit (radio station)**		military and non-military intelligence, decryption of communications; radar surveillance	yes		

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
UNITED KINGDOM	**Government Communications Headquarters (GCHQ)** reports to the Foreign Secretary	*Intelligence Services Act 1994*	counter-intelligence/ overseas intelligence; SIGINT in the poltical, economic, scientific/technological and military fields	yes	*The Security Service Commissioner* is appointed by the Prime Minister and is either a serving or retired senior judge *The Investigatory PowersTribunal* *Intelligence and Security Committee* The Committee consists of nine members (House of Commons + House of Lords, none of whom may be a Minister of the Crown) appointed by the Prime Minister	*In Ac* *In Ac* *In Ac*
	Secret Intelligence Sevice (SIS) = MI6 reports to the Foreign Secretary	*Intelligence Services Act 1994*	gathering information on intelligence activities and political events abroad			

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
UNITED KINGDOM	**Security Service = MI5**, reports to the Home Secretary	*Security Services Acts 1989 and 1996*	intelligence gathering to safeguard internal security; counter-intelligence, counteracting extremist movements (including the IRA), Terrorism, and subversive elements		*Security Service Commissioner* *Intelligence and Security Committee*	*Se 19* *In Ac*
UNITED KINGDOM	**Defence Intelligence Staff (DIS)** reports to the Minister of Defence		supporting military security; evaluating and analysing military, political, technical/scientific and selected economic information			

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
USA	**Central Intelligence Agency (CIA)**	*National Security Act 1947*	world-wide intelligence gathering; counter-espionage abroad, central responsibility for all intelligence matters in the USA		*Senate*: *Senate Select Committee on Intelligence (SSCI)* *House of Representatives: House Permanent Select Committee on Intelligence (HPSCI)*	es ba de re *In Ac* H. 95 es ba of R 17 in *O*

USA	**Defense Intelligence Agency (DIA)**	established by the 1961 *Directive 5105.21* by the Defence Secretary *Executive Order 11905* of 1976 *DoD Directive 5105.21 1978 Executive Order 12036* *1981 Executive Order 12333*	responsible for supplying military intelligence für intervention forces and decision-makers in the Defence Ministry and in the Government		*Senate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI*	se

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
USA	**National Security Agency (NSA)**	*Executive Order 12333 of 4 December 1981*	responsible for the security of US Intelligence systems, especially decryption; responsible for interception of communications abroad	yes	*Senate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI)*	se
USA	**National Imagery and Mapping Agency (NIMA)**	*National Imagery and Mapping Agency Act of 1996.*	responsible for supplying images and maps and for analysing them;		*Senate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI)*	se
USA	**National Reconnaissance Office (NRO)**		responsible for the development and use of satellite espionage systems (SIGINT, images)		*Senate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI)*	se

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
USA	**US Army Intelligence (e.g. Deputy Chief of Staff for Intelligence), Intelligence and Security Command (INSCOM)**	*Executive Order 12333* (December 4,1981)	Intelligence gathering and analysis in the military sphere; development of concepts und systems for military intelligence und electronic warfare	yes	*Senate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI)*	se
USA	**Marine Corps Intelligence Activity (MCIA)** **National Maritime Intelligence Center (NMIC)**	*Executive Order 12333* (December 4, 1981)	Naval intelligence; military reconnaissance and development of decryption and electronic warfare support systems	yes	*Senate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI)*	se
USA	**Office of Naval Intelligence (ONI)**	*Executive Order 12333* (December 4, 1981)	intelligence für Navy and maritime issues, Analysis of foreign fleets, collecting data about ocean surveillance systems and about submarine platforms and weapons systems	yes	*Senate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI)*	se

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
USA	**Air Intelligence Agency (AIA)**	*Executive Order 12333* (December 4, 1981)	airforce intelligence for airforce, military reconnaissance	yes	*Senate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI)*	se
USA	**Federal Bureau of Investigation (FBI)**	*Title 28, United States Code (U.S. Code)*, Section 533 established in 1908; under this name since 1935.	counter-intelligence federal police force;		*Senate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI)*	se
USA	**Drug Enforcement Administration**	*Executive Order of July 1, 1973*	collecting intelligence about drugs and money-laundering abroad		*Senate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI)*	se

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
Canada	**Communication Security Establishment (CSE);** is supported by the **Canadian Forces Supplementary Radio System (CFSRS)**	Formal mandate constitutes classified information but is probably approved by the Cabinet	Advises government and business about security issues relating to data transmission and processing (Infosec), development of encryption systems	yes	no independent control authority (subject solely to monitoring by the Auditor General and the Minister of Defence who is accountable to Parliament)	(1 *Ac*
Canada	**Canadian Security Intelligence Service (CSIS)** reports to the Minister of the Interior	*Canadian Security Intelligence Service Act (CSIS Act)* aus 1984	counter-espionage, combating sabotage and international terrorism in Canada		**The Security Intelligence Review Committee (SIRC)** independent body consisting of 5 members who may not be Members of Parliament	*Ca* *In* *Ac*
Canada	**Director General Intelligence Division** (under the *Deputy Chief of the Defence Staff)* reports to the Minister of Defence		intelligence in the military sphere			

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
Australia	**Defence Signals Directorate (DSD**) reports to the Minister of Defence		collecting and disseminating signals intelligence; supplying information security products (Infosec) for the Government and for the military		*Inspector General of Intelligence and Security (IGIS)* (appointed by the Prime Minister)	In In Se
Australia	**Defence Intelligence Organisation (DIO)** reports to the Minister of Defence		collecting and analysing strategic and military information und intelligence		*Inspector-General of Intelligence and Security (IGIS)*	se
Australia	**Australian Secret Intelligence Service (ASIS)** foreign intelligence service reports to the Foreign Minister		collecting foreign intelligence, with particular reference to South-East Asia in the interests of national security, business and external relations		*Inspector-General of Intelligence and Security (IGIS)*	se

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
Australia	**Australian Security Intelligence Organisation (ASIO)**	*The Australian Security Intelligence Organisation Act 1979 (the ASIO Act)*	protection against politically motivated violence; personal and material security combating international terrorism and illegal technology transfer		*Parliamentary Joint Committee on the Australian Security Intelligence Organization* *Inspector-General of Intelligence and Security (IGIS)*	Se AS se
Australia	**Office of National Assessments** independent body	*Office of National Assessments Act 1977*	reports to the Prime Minister		*Inspector-General of Intelligence and Security (IGIS)*	se

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
New Zealand	**Government Communications Security Bureau (GCSB)** reports to the Prime Minister	established in 1977 no legal basis to date, but a bill is currently before Parliament (*Government Communications Security Bureau Bill*)	securing information about foreign countries; communications security, computer and information security (Infosec); technical security	yes	*Inspector-General of Intelligence and Security* *Intelligence and Security Committee* (Prime Minister, Leader of the Opposition, 3 MPs)	*Th of Se* *Th Se Ac*
New Zealand	**New Zealand Security Intelligence Service (SIS)** internal intelligence service reports to the Prime Minister	*New Zealand Security Intelligence Service Act 1969*	counter-intelligence, protection against terrorism and politically motivated violence, raising awareness in scientific research and industry to the problems of industrial espionage and illegal technological transfer			
Country	**Intelligence service**	**Legal basis**	**Duties**	**SIGINT capacity**	**Control authority**	**Le**
New Zealand	**External Assessments Bureau (EAB)** foreign intelligence service reports to the Prime Minister		analyses political developments and draws up reports on political and economic events and trends			
New Zealand	**Directorate of Defence Intelligence and Security (DDIS)**		military intelligence service; collects data relevant to the military, above all in the Asia-Pacific			

	military intelligence service reports to the Minister of Defence		area; analysis of tactical and strategic information			