On Globalisation of Control: Towards an Integrated Surveillance System in Europe

Thomas Mathiesen
Professor of sociology of law, University of Oslo

A Statewatch publication

Thomas Mathiesen, born 1933, since 1972 professor of sociology of law at the University of Oslo, Norway. He has done research and published a number of books in a wide variety of areas such as sociology of law, criminology, political sociology and sociology of the media. He was one of the founders of the Scandinavian prison movement, where he is still active. In addition to the Scandinavian languages, many of his books and articles have been published in English, German, Italian, Portuguese, French and Japanese. His last book in English, Prison on Trial from 1990, will appear in a revised and updated edition in 2000. In recent years he has been actively engaged in research on the new European surveillance systems, and written a book and many articles on the topic in Norwegian. This is his first publication in English on the topic. He was actively engaged in the attempt to keep Norway outside the Schengen agreement.

A Statewatch publication, November 1999

Printed by Instant Print West One, 12 Heddon Street, London W1R 7LJ

Further copies are available from:
Statewatch,
PO Box 1516,
London N16 0EW,
UK

tel: (00 44) (0)181 802 1882 fax: (00 44) (0)181 880 1727 e-mail: office@statewatch.org

Preface

During the past thirty years, the Western world has seen a tremendous development in information technology. The technology has changed our lives. But while we easily grasp the bright side of the information technology – the mobile telephones we can avail ourselves of, the computers we can use, the Internet where we search for information and (mostly?) entertainment – information technology also has a dark, dangerous side. Never in the history of mankind has there been a technology which so clearly has had a "double character" (to borrow an expression from Marx). The dark side comprises the use of the sophisticated and rapidly advancing technology for *surveillance purposes*, a surveillance which quickly is coming to a point where it threatens the democratic fibres of our societies.

This paper is written as a warning against this dark, dangerous side. Both state and private sectors engage in widespread surveillance based on modern information technology. In this paper, I deal only with the engagement of the state, notably the numerous surveillance systems used for policing purposes. The purpose is to give an overview and a generalised interpretation. The engagement of the state is particularly dangerous because it is to a large extent clouded in secrecy, and because we do not recognise it in our daily lives. It contains a power which is very different from (but supplementary to) the open physical, even violent police power which we have inherited from the past. It is precisely because of its hidden, unnoticed character, that it is so dangerous: Its hidden character pulverises resistance and prevents it from coming on the agenda of public attention.

I wish to thank the editor of *Fortress Europe?*, Nicholas Busch, the editor of *Statewatch*, Tony Bunyan, and Dr Heiner Busch for extremely valuable comments and for constructive criticism. In the case of Nicholas Busch, the comments and criticism have concerned various drafts and articles (and a book) which I have written on the topic in my native language, Norwegian, and which constituted an important background for this paper in English. All three have generously shared information with me. But I alone am responsible for any errors or shortcomings.

Thomas Mathiesen

"Campsfield detention centre, near Oxford, has 20 foot metal fences topped with razor wire, electronic gates and video cameras inside and out. A Belgian centre for asylum-seekers has razor wire and isolation cells 'to allow troublemakers to cool off' according to the interior minister. He responded to administrative court denunciations of conditions in asylum centres as inhuman and degrading, 'It won't be the last time'. In France, cells in the basement of the Palais de Justice for asylum and immigration prions, were condemned and 26 detainees released by a horrified judge in March 1995 after a series of violent incidents including beating and attempted rape by guards, and a suicide. In Germany, there have been repeated allegations of police brutality towards asylum-seekers ... containers, bunkers and camps which were pressed into service as 'collection camps' in 1991-2. In the Dutch detention centre of Grenshospitium, Jacqueline Mulata died for want of medical attention; and in Pentonville prison, Omasase Lumumba, great-nephew of Patrice Lumumba, was unlawfully killed by prison officers. ..."

Frances Webber, 1995

In 1985, Germany, France and the Benelux countries entered an agreement in the little town of Schengen in Luxembourg. The agreement, which was formulated in general terms, aimed at mutual recognition of visas between the countries and strengthened police cooperation. The major point of the agreement was to abolish national border controls between the countries, while at the same time strengthening controls along common external borders. Strengthened police cooperation was envisaged as a method of enhancing the external border controls as well as making up for the internal "deficit" created by the disappearance of national border controls.

In 1990 the same five countries entered a new agreement, again in Schengen. This agreement, which is usually referred to as the Schengen Convention, is a convention implementing the Schengen agreement of 1985. It regulates a long series of crucial questions concerning national and common external border controls, police cross-border "hot pursuits", police cross-border data cooperation, including registration of persons and objects, and so on. In effect, the convention opens for wide ranging registration and surveillance of large population groups in the countries concerned.

Full membership in the Schengen cooperative arrangement has always been restricted to EU-countries. Until 1999 the Schengen Convention was an inter-governmental agreement outside the EU, and the individual member state had the right of veto. After the convention was signed by the original five countries, Italy, Spain, Portugal, Greece and Austria joined the agreement. Great Britain and Ireland stood outside, wanting to maintain their national border controls intact.

An important change in Schengen matters took place in 1999. At the EU summit in Amsterdam in June 1997, which concluded a lengthy conference with complicated negotiations (de Zwaan 1998) between the governments of the EU countries, the EU ministers decided to integrate the Schengen system, lock, stock and barrel, into the EU structure, partly in the first (supranational) pillar and partly in the third (inter-governmental) pillar. The Schengen Executive Committee was to be supplanted by the Justice and Home Affairs Council (JHA) in the EU structure. The Amsterdam Treaty was signed by the foreign ministers on 2 October 1997, and entered into force on 1 May 1999.

The integration of Schengen in the EU structure will give the various Schengen arrangements, including the vast data-based registration and surveillance system, added momentum and influence. In addition, the "disappearance" of the whole Schengen arrangement into the fragmented hundreds of EU-bodies and work groups, and among the tens of thousands of intricate EU documents, will make the Schengen activities, which have been difficult enough to monitor as separate Schengen activities, even more hidden and almost impossible to scrutinise and criticise - at least for outsiders.

The Nordic EU member states – Finland, Sweden and Denmark – have also ratified Schengen within the EU, and the Nordic non-EU members – Norway and Iceland – have entered a so-called "agreement to collaborate" in Schengen matters with the EU (the latter countries do not have access to the EU decision-making bodies, but are members of a so-called Joint Committee outside the EU structure, and may make suggestions and proposals, but do not have the right to vote). At the time of writing, Great Britain and Ireland still stand outside, but on 20 May 1999 the two states formally applied for participation in some of the Schengen activities, notably those related to law enforcement,

including participation in the joint data-based registration and surveillance system. The application was made pursuant to Article 4 in the Schengen protocol of the Amsterdam Treaty, and was favourably received by the JHA Council.

Through Schengen, then, a widespread system and network of police cooperation, data registration and surveillance - from Iceland in the North to the Mediterranean in the South, and from the tip of Portugal in the West to the German/Polish border in the East - is in the making, and is a reality as the 2000s begin.

Space forbids discussion of all aspects of the Schengen system; such a discussion requires a book in itself (Mathiesen 1997 a). In this paper, I will concentrate on the cross-border, data-based registration and surveillance system, with its auxiliary supplementary information exchange, which has been operative since 1995 in the Schengen states. After having reviewed the major Schengen institutions and issues relevant to this, I will move on to discuss some of the many other data-based registration and surveillance systems which are in the making within the EU. On the way and towards the end of the paper, I will raise the question of whether we are moving towards an extensive, integrated registration and surveillance system - a vast, amalgamated police-based data system, with various specialised branches, which, if this is the developmental direction, may function both on the individual and the aggregate level: Individuals may be subjected to particular scrutiny, while large population groups may quickly be sorted out for surveillance and "special treatment".

The development which seems to be ahead, is another aspect of the so-called globalisation process which currently is taking place in economics, politics, and so on. *At present police control is also globalised, based on advanced information technology.*

Bureaucratic registers have been used for both of the above-mentioned purposes - individual and aggregate registration, surveillance and "treatment" - before in European history. On the individual as well as the aggregate level, the fate of the Jews and other population groups in the 1930s and 1940s is a case in point, and there are many other examples.

An excellent - and tragic - concrete example, is the way in which the Germans occupational forces in Norway during World War II used various existing registers, established for other purposes, in persecuting the Norwegian Jews. Over 50% of the 1,400 Jews in Norway in 1942 were exterminated, while the figure for Denmark was under 1% out of 5,600 (and under 0.5 % out of 2,300 for Finland). Why the much higher percentage for Norway? There are several reasons, one of them being that Norway had excellent registers pertaining specifically to Jews.The Norwegian Constitution of 1814 barred the entry of Jews to Norway, a prohibition which was abolished in 1851, but as a kind of substitute, separate registration was undertaken: From 1866 on, the Norwegian Census Bureau specifically registered Jews as a separate group of dissenters. The census was useful for German occupational forces and for the Norwegian nazis. The register of the Norwegian Radio Authorities also proved useful: In 1940, right after the German invasion, the German authorities ordered the radios belonging to Jews living in the capital city to be confiscated. The radio authorities had a register which could be used for the purpose. Consequently, the Jews themselves could also be tracked down (Sørbye 1998).

Bureaucratic registers may be used for such purposes by police forces out of control, but also by political authorities when the political wind is right and the time is ripe, as was the case in Norway during World War II. The new, technically extremely innovative, combinable, hidden and cross-border uncontrollable data-based registration systems which are presently rushing forward, constitute an increased, enormous threat which cannot be ignored by anyone preoccupied with police and political control after 2000.

I will start the account with Schengen because the Schengen data system for registration and surveillance is rather solidly on wheels, while the other systems are in the planning, drafting or ratification stage. As I will expand on later, for this reason Schengen is a kind of "centre of gravity" among the various systems. However, as the other systems become operative, Schengen's centrality may be reduced, and other systems may take its place as "leading stars". In particular, what is known as Europol, with The Europol Computer Systems, may take on the leading role, with power and communication lines to the other systems. More about this later.

In Schengen: SIS

In order to strengthen common external border controls as well as to make up for abolition of national borders, the Schengen Convention opens for various types of covert police action, and cross-border police collaboration concerning such actions. Examples of collaborative covert police actions are contained in Articles 40 and 41 of the convention.

Article 40 authorises "observation" (the Swedish and Danish translations of the convention simply say "surveillance") across national borders of persons "presumed to have taken part in a criminal offence to which extradition may apply". "Presumed" to have "taken part in" a criminal offence to which extradition "may apply" are broad terms, and the provision is wide and vaguely delimited. Officers conducting the observation may not challenge or arrest the person under observation. In 1996, observation across national borders was used in 135 cases within the Schengen territory[1]; in 1997 the number had increased to 371.[2] Article 41 authorises "continue[d] pursuit" across national borders of individuals "apprehended" in the act of committing or participating in one of a series of specified offences. The foreign officers may apprehend the individuals in question until the local police takes charge. In 1996, continued pursuit was used in 39 cases.[3] The figures will almost certainly increase with time. Article 40, which vaguely authorises cross-border "observation", constitutes the greatest threat to the legal protection of individuals.

However, provisions such as these are peanuts compared to the comprehensive *data system* which is developing. The data-based collaborative system between the national police forces of the Schengen states has entirely different dimensions, and has already - as we shall see - hundreds of thousands of individuals "on file".

As alluded to already, inside Schengen there are two comprehensive registration- and surveillance systems in operation and continual development: A data-based registration and surveillance system, and an auxiliary system for supplementary information exchange. The first is called Schengen Information System or SIS. Article 93 of the Schengen Convention states the purpose of SIS:

> *The purpose of the Schengen Information System shall be in accordance with this Convention to maintain public order and security, including State security, and to apply the provisions of this Convention relating to the movement of persons, in the territories of the Contracting Parties, using information transmitted by the system.*

As the provision shows, the stated purpose is very wide and comprehensive, comprising *both* "public order" *and* "State security". No further definitions of these terms are given, which means that just

---

[1] Source: Report from the German Ministry of the Interior about the Schengen Cooperation in 1996, delivered to the Federal States 5/6 June 1997; as reported in *Statewatch* July-October 1997, p. 3.

[2] Annual Report for 1997 from the Schengen Executive Committee; as reported in *Statewatch* May-August 1998, p. 28.

[3] Source: as above for "observations" in 1996. It is of some interest to note how far a given state may go to bring Schengen provisions like these in line with national legislation. In a letter to the Norwegian Ministry of Foreign Affairs (2 September 1998), the Norwegian Ministry of Justice noted that foreign police forces may not execute police authority in Norway, and that the Schengen convention does not overrule this. But, the letter continued (with special reference to article 41), foreign police forces may be given authority to apprehend people on Norwegian soil pursuant to the general authority, which is given by law in Norway, that the police *or* "any other person may apprehend a suspect caught in the very act or on the basis of fresh tracks". The implication is that Swedish or Finnish police officers cannot cross the border to Norway *as police officers* in order to apprehend, but can do so as *any other person*, that is, as civilians. The further implications of this are rather ludicrous. Is the foreign police officer supposed to change into civilian clothes at the border? Which police officer carries civilian clothes with him when engaged in a hot pursuit? Is he supposed to undress and cross the border naked? In that case, the Norwegian police would certainly take care of him. On top of it all, according to article 41, 5 d in the Schengen convention, the pursuing officers "shall be easily identifiable", for example by an armband, and "the use of civilian clothes ... without the aforementioned identification is prohibited". The proposal in question was not upheld, and a new legal basis was provided in the Police Act instead, but in any case it shows how far a state may go to accomodate Schengen rules and decisions.

about everything may be included, from acts of qualified terrorism through various forms of social unrest to political demonstrations deemed to be a threat to public order and/or State security by the governments concerned.

Broadly speaking, the information which may be stored in the system may be viewed in terms of three major levels or tiers. Firstly, Article 94.3 of the convention specifies the items which may be included in respect of persons: name and forename, and any aliases possibly registered separately; any particular objective and permanent physical features (an example would be skin colour); first letter of second forename; date and place of birth; sex; nationality; whether the persons concerned are armed; whether the persons concerned are violent; reason for the report; and action to be taken. In other words, the basic information combines objective (sex) and evaluative (estimated violence) items.

But this is just the beginning. The second tier concerns who or what may be registered, and begins with Article 94.1, which stipulates that the items of information may only be supplied when this is required for the purposes laid down in Articles 95 to 100. Articles 95 to 99 refer to persons, while Article 100 refers to objects. Article 95 refers to persons wanted for arrest for extradition purposes; Article 96 refers to aliens who are reported for the purposes of being refused entry ("unwanted aliens"); Article 97 refers to persons who have disappeared or persons who, "in the interests of their own protection or in order to prevent threats", need to be placed provisionally "in a place of safety" (!)[4]; Article 98 refers to witnesses (!), persons summoned to appear before the judicial authorities in order to account for acts for which they are being prosecuted, or persons who are notified of a criminal judgment or of a summons to serve a custodial sentence; Article 99 refers to persons who, in compliance with national law, are to be subjected to "discreet surveillance" (!) or "specific checks".

The third tier provides the conditions under which a person may be subjected to "discreet surveillance" (under-cover investigation) pursuant to Article 99, and the information which may be communicated about a person to the police of another country who has entered an alert for discreet surveillance in the SIS about the person. Article 99.2 provides some of the conditions under which discreet surveillance may be used. They are partly rather precise, and partly extremely vague, opening for discreet surveillance of broad categories of people. Thus, the general introduction to Article 99.2 states that "[s]uch a report may be made for the purposes of prosecuting criminal offences" - a reasonably (though not wholly) precise stipulation. But then the general introduction continues: "...and for the prevention of threats to public safety" - a very vague stipulation to say the least.

The same mixture of preciseness and vagueness may be found further on in Article 99.2. On the one hand, discreet surveillance may be used

> *where there are real indications to suggest that the person concerned intends to commit or is committing numerous and extremely serious offences,...*

This is a fairly precise stipulation. But then the text goes on to say

> *...or where an overall evaluation of the person concerned, in particular on the basis of offences committed hitherto, gives reason to suppose that he will also commit extremely serious offences in the future.*

This is a vague and open stipulation ("overall evaluation", "gives reason to suppose"), in addition to being exclusively oriented towards possible - quite hypothetical - future acts.

Furthermore, and most importantly, Article 99.3 opens for discreet surveillance of political behaviour. Article 99.3 states that "a report may be made in accordance with national law, at the request of the authorities responsible for State security". In Norway, "authorities responsible for State security" is equivalent to the Secret Police. Such reports may be made when "it is necessary for the prevention of a serious threat by the person concerned or other serious threats to internal or external

[4] (!) Author's comment.

State security". There is not one word in Article 99.3 about offences or qualified criminal acts. The procedure to be followed by "the authorities responsible for State security", when requesting discreet surveillance, is detailed in a secret manual, to which I shall return later.[5]

Article 99.4 stipulates the information which may be communicated about a person to the police of another country who has entered an alert for discreet surveillance in the SIS about the person. The information includes persons accompanying the person concerned (!) or occupants of the vehicle (!). The Norwegian translation of the convention makes clear what the latter term means: Passengers.

In short, the background for storing information in the SIS is wide and discretionary, many items of information are evaluative, and "discreet surveillance" quite clearly opens for political surveillance and surveillance of a wide circle of individuals around the main person.

The Schengen Information System has a central data base in Strasbourg, and national SIS-bases in all of the Schengen states. The national data bases are supposed to have identical information stored, and this information is in turn supposed to be identical with the information stored in Strasbourg. In 1995 altogether 30,000 computers throughout the seven Schengen states which at that time were on-line had access to the SIS through their national SIS bases. In 1997 the number of access points throughout the nine states which then were on-line was approximately 48,700.[6] The number of records ("*gespeicherten daten*", "record entries") stored on 26 March 1996 was close to 3,9 million. Germany and France were the large users.[7] Information was stored about hundreds of thousands of persons, and the capacity of the system was at that time estimated to be 9 million records. For each succeeding year the numbers went up, from 5.6 million in 1997 to over 8.8 million in 1998. The figures are based on the total number of record entries in the SIS on a single day (for 1998: 5 March), and do not reflect the numbers deleted or added during the course of a year.[8]

In any event, the system is very large. And primarily due to the increasing number of states joining Schengen, it will become larger: Expansions are in the making - further development and technical up-grading of the central SIS-base in Strasbourg, final integration of the Nordic countries into the system, increased number of links between SIS and numerous other European registration systems, and the like.[9] The report, mentioned in note 1, from the German Ministry of the Interior about the Schengen Cooperation in 1996, delivered to the Federal States 5/6 June 1997, has this to

---

[5] The secret manual, the so-called "SIRENE manual", is only one example of the general secrecy with which Schengen's development is imbued. Whole series of important documents have for long periods of time been secret, unavailable or extremely difficult to get hold of. Consequently, it requires great effort to get under the skin of the system. The system is a "hidden" system in a very real sense of the word. As a small example, I may mention that in October 1998, pending the renewed negotiations between Norway and the EU concerning a new agreement of cooperation with the "new Schengen" inside the EU, the National Norwegian Broadcasting Company asked the relevant Norwegian ministers for about 100 documents relevant to Schengen. They were denied access to 63 of them -- almost 2 of every 3 documents.

[6] Sources: Report from the German Ministry of the Interior, fall 1995, and *Statewatch European Monitor*, Vol. 1 No 1, 1998, p. 30, with full text reference to Report dated 25 September 1997 from the SIS Steering Committee.

[7] Source: The annual report of 26 March 1996 from Schengen's Central Group.

[8] The Annual Report for 1997 from Schengen, as reported in *Statewatch* May--August 1998, p.27; the figure for 1998 as reported in *Statewatch* May—August 1999, p. 22. The figure for 1998 includes 1,2 million personal data entries and 7.6 million entries relating to objects. As a result of the high number in the so-called alias groups, that is, people who have a false second identity, "only" 795 000 of the 1,2 million personal data entries match actual people. Almost 5,3 million – 70 % -- of the 7,6 million entries relating to objects concerned lost or stolen ID papers. Only about 13 % of the entries relating to objects concerned vehicles, and other objects – banknotes, firearms etc. – showed even smaller percentages (only 2—3 % concerned firearms; source of statistical information: *Statewatch* May—August 1999, p. 23). In other words, a vast majority of the entries concerned unwanted aliens, deportation matters, lost identity papers and so on, and not qualified crime. I will return to this point below.

[9] Sources: Work Programme of the Austrian chairmanship in Schengen, fall 1997, p. 8; see also minutes from the meeting of 7 October 1997 in Schengen's executive committee as well as *Information News Letter: Information for People Working in the Ministry of the Interior*, No. 1 Sept. 1997 p. 3.

say about the integration of the Nordic countries.[10]

> *[I]t has been decided to redesign the SIS completely in order to integrate the five Nordic states. The integration of the Nordic states will follow in a second technical generation of the SIS. This new SIS II will be designed in a way that the integration of future member states (eg within the framework of an enlarged EU) will be technically possible at any time.*

The Work Programme of the German chairmanship in Schengen, fall 1998 (p. 8 in the Danish translation) goes on to distinguish between a so-called *SIS I plus* plan – an upgrading of the present SIS, including integration of the Nordic countries – and *a SIS II* plan, implying a new structure on the basis of experiences with the present SIS, including plans for the integration of central and eastern European countries as the EU moves its external border eastwards.

The fantastic magnitude of the whole project is more than apparent.

In Schengen: SIRENE

SIS, however, is only one of the systems for information exchange in Schengen. The other system is called *SIRENE*, an abbreviation for *Supplément d'Information Requis a l'Entrée Nationale* (Supplementary Information Request at the National Entries). SIRENE is intended to facilitate bilateral and multilateral exchange, mainly of supplementary information about persons and objects registered in the SIS, between the national police authorities in different Schengen countries. *Fortress Europe?* comments on the SIRENE system as follows (December 1996-January 1997, p. 5):

> *SIRENE could best be described as a complex, network-like structure for bilateral and multilateral police and security cooperation between the Schengen countries, including central national offices and a sophisticated computerised information system, enabling the exchange of 'supplementary' data on persons and items prior to the entry of a report in the SIS, or following a hit (positive search) in the SIS.*

Through the SIRENE system, police authorities in one country who have arrested a person who is registered in the SIS by another country, may require supplementary information, not stored in the SIS, from the latter country. The SIRENE system has developed alongside SIS, and is far less known and not even mentioned in the Schengen Convention.

The system *is*, however, mentioned in a draft convention intended for the European Information System, EIS, within the EU. We shall return to EIS later, here only this: the draft convention clearly shows that the SIRENE is designed for exchanging information which is extremely broad and virtually without limits. After having explicitly stated that each of the member states shall establish a SIRENE office with central responsibility for the exchange of supplementary information, the draft goes on to say (my emphasis):

When a report is included or action to be taken is performed, the SIRENE offices shall exchange, in compliance with this Convention and their national law, such further information as is necessary to identify the persons or objects reported as well as other information and documentation relevant to the follow-up action taken.

SIS, after all, stores fairly limited and standardised items of information. The national SIRENE units, on the other hand, handle far-reaching, non-standardised information or "soft" data. "[S]uch further information as is necessary", and "other information and documentation relevant", are highly imprecise, all-embracing concepts or terms, which may include almost everything. This is also explicitly pointed out by people working in the SIRENE offices. The director of the Portuguese SIRENE office boasted of the SIRENE system in the following words on Norwegian television 10

[10] Source and translation: *Statewatch* July-October 1997.

March 1997 (translated from the Norwegian subtitles by the author):

> *The convention stipulates who has access to the system. But generally speaking, the police has access. They are, of course, at the airports, in the seaports, and can intercept mobile phones. It follows that they have access to masses of information all the time. They don't need to look for faxes. This is a rapid system. It is updated. There are masses of information. And naturally the efficiency of the system is much greater than that of the traditional Interpol system.*

The police intercept mobile (and other) phones. The information is exchanged between the SIRENE offices. The working language of the SIRENE-bureaus is English, not a language of any of the Schengen countries, therefore also called "Schenglish" (Tromp 1998). Those working in the SIRENE view communication as the key task:

> *Communication is in fact the key word for SIRENE. It is not only a matter of exchanging forms and contacting other bureaus, but, particularly on the national level, there is a great need of communication. Take for example the coordination between SIRENE and the public prosecutors; but also between SIRENE and all the organisations dealing with different types of alerts, such as immigration services, border-authorities, police, ministries of justice and, internal affairs and last but certainly not least, technicians* (Tromp 1998, p.2).

Communication is SIRENEs main task. Communication of information between the police in different states has been on the increase for several decades. The SIRENE system formalises and legitimises the activity, thus greatly strengthening it. There exists a comprehensive manual for the SIRENE. As mentioned already, the manual is secret (confidential),[11] but major parts as well as summaries have leaked out and have already been published (see e.g. *Fortress Europe?*, December 1996/January 1997).

The SIRENE manual postulates that (all quotes translated by the author from the Danish version) the "[E]xchange of information through for example photographs or finger prints may prove to be decisive". According to the manual, communication between the SIRENE offices may be oral or written, as well as through pictures (photos, fingerprints). The communication of texts and pictures through the SIRENEs own electronic mail system is preferred over other means of telecommunication, and wherever possible, oral communication by phone should be used. Oral communication and communication through the SIRENEs own electronic system leave fewer traces. The SIRENE offices are required "to answer requests from the other Contracting Parties as quickly as possible. The time should not exceed 12 hours" (p. 26 in the manual).

Clearly, the SIRENEs also transmit information other than supplementary information to the SIS. On p. 39 the SIRENE manual says: "The cooperation between the Contracting Parties and competent authorities of the police cannot just be limited to use of the information in the Schengen Information System". Furthermore, the manual says: "- [T]he SIRENE offices of the Contracting Parties may exchange all necessary information, in compliance with national legislation, pursuant to Articles 39 and 46". Articles 39 and 46 of the Schengen Convention, which the SIRENE manual refers to here, are not relevant to the SIS, but goes beyond the SIS to mutual assistance in general between police authorities of the Contracting Parties for the purpose of preventing and detecting

[11] The SIRENE manual is a part of the Schengen *acquis* -- over one thousand pages of binding decisions and declarations made by the Schengen Executive Committee. The comprehensive manual is, along with some other parts of the *acquis*, secret pursuant to a decision made by the Executive Comittee of 14 December 1993 (itself a part of the *acquis*, and thus binding to the participating states). The decision states that the manual (along with the other relevant parts of the *aquis)* "shall" or "should" (from the French "doivent", in the intermediate zone between "shall" and "should") remain confidential "[i]ndependently of the different national rules". This decision, which has largely remained unnoticed, is actually sensational: By internal decree it obliges the participating states to keep the relevant documents secret *regardless of what national legislation has to say about the matter*. Citations from the Schengen *acquis* are translated from Norwegian or Danish texts by the author.

criminal offences (Article 39), and to the sending - without being asked - of "any information which may be of interest to [the Contracting Party concerned] in helping prevent future crime and to prevent offences against or threats to public order and security" (Article 46.1).

Clearly, the range of application of the latter stipulation in particular is very wide indeed. Firstly, reference is made to "helping prevent future crime" - an imprecise category indeed, which implies that no concrete suspicion is necessary. Secondly, reference is made to "prevent offences against *or* [my italics] threats to public order and security". The word "or" indicates that the range of application *goes explicitly beyond any reference to offences or crimes whatsoever.*[12] The article therefore opens for bilateral/multilateral exchange of information concerning highly diffuse matters, matter which may certainly include political activities when defined as a threat. *Fortress Europe?* makes this telling comment (December 1996-January 1997, p.5):

> *Compared with the amount and sensitivity of information that can be stored and exchanged by the SIRENE offices, the SIS is actually little more than an index system.*

Like SIS proper, the SIRENE system is undergoing continual expansion. The Work Programme of the German chairmanship in Schengen, fall 1998 (p. 9 in the Danish translation) has this to say about plans for the SIRENE system: "[M]odernisation and acceleration of information exchange on the basis of the final implementation of the SIRENE network, phase II".

To summarise, the SIRENE system is a complex information system concerning far-reaching, non-standardised information which supplements the SIS, but which also lives its own life independently of the SIS, and which is oriented towards something as general as public order and security, well beyond activities supposed to be criminal. When we recall that Articles such as 93 and 99.3, referred to above, open for similar exchange of undefined information within the SIS, we envisage a total system which may and does go far beyond even such a highly diffuse matter as "prevention of crime".

More about this in the following.

In Schengen: Crime Prevention?

Above we have largely presented Schengen's goals and possible range of activities as they can be sifted from a reading of the Schengen Convention and other generalised Schengen documents. As we have seen, the convention and the other documents open for several possible lines of actual development of the Schengen collaborative effort. Do we have empirical data, or concrete documentary information, which indicate what concrete road or roads Schengen is on?

A number of times, Norwegian authorities have stated that Schengen's purpose is the combating of traditional, serious international crime. So have the Schengen authorities themselves. For example, according to the Work Programme of the Austrian chairmanship in Schengen, fall 1997, one of three prioritised tasks would be "to pursue as concretely as possible" the joint action against international crime.

The facts are different. Statistical information from Germany as well as statistical information and reports from Schengen itself, show that the Schengen system of cooperation to a very large extent is focused on *identity papers and unwanted aliens*, such as asylum seekers who have been refused entry and have gone underground.

*

For one thing, this is apparent when we look in more detail at the above-mentioned (note 6) Report from the German Ministry of the Interior, fall 1995. The report showed that close to 70 % of the 2.3 million records ("datenzätze") which up to that time were entered in the SIS by Germany alone,

[12] The crucial word "or" appears not only in the English translation of the convention, but in the French original text as well as in all of the Scandinavian translations.

concerned unwanted aliens and identity papers. Of the 2.3 million records, about 700,000 concerned persons. Of these, 600,000, or about 86%, were registered pursuant to Article 96 in the Schengen Convention, concerning aliens who are reported for the purposes of being refused entry. Some of these may have committed serious, traditional crimes. But surely not the majority: The same report reviews the SIRENE system, which is more detailed, and which indicates that the aliens to a large extent were asylum seekers who had been refused entry in Germany, and who had gone underground (for further details, see Mathiesen 1997 a, p.51).

Similarly, a closer look at the Report from the German Ministry of the Interior about the Schengen Cooperation in 1996, delivered to the Federal States in June 1997 (see note 1), shows that of the 4.2 million requests for information during 1996 mentioned earlier, 62% concerned unwanted aliens or identity papers. The second largest category were requests concerning motor vehicles, which amounted to 20% (a few projects have been launched specifically concerning control of motor vehicles, with very meagre results as far as stolen cars goes; furthermore, requests about motor vehicles of course do not necessarily aim at criminal conduct). The third largest category concerned forged bills, which amounted to 13%, while 4% were requests concerning weapons. Of the 4.2 millions requests that year, over 476,000 concerned persons. Of these, 413,000, or 88 %, were requests pursuant to Article 96 concerning unwanted aliens. The Annual Report of the Central Group in Schengen, dated 26 March 1996 (see note 7) is somewhat less clear because of ambiguities in data collection, but it gives the same overall picture.

The Annual Report on the State of Affairs along the External Schengen Border during 1996, published 20 March 1997, tells the same story, only more clearly so. The report points to several technical problems relating to border controls, especially at seaports (less so at the airports), and details some of the problems for the individual countries. By way of introduction, it emphasises the struggle against cross-border crime and illegal immigration as two functions of the external border control. *When going into detail, however, the report says nothing about serious control of cross-border crime.* Rather, the returning of third country citizens to third countries, the control of visas, forged documents and so on are reported. Crimes in a traditional sense may be hidden in this material, but they are hardly conspicuous. A total of 563,423 control actions are reported at the external borders, 41 % concerned refusal of entry from third countries, 28.5% concerned third country citizens apprehended without a residence permit near the border, 24.5% concerned the returning of third country citizens to third countries, 3% concerned third country citizens in the possession of forged documents and 0.5% concerned "apprehended people smugglers" ("festgenommenen Schleuser"). 4.8% were unclassifiable due to unreadable report. It appears abundantly clear that *the crux of the matter is a policy of shutting out aliens.* It also appears that in so far as the apprehension of organised people smugglers is a Schengen goal, Schengen border control are a complete failure.

The fact that the crux of the matter is a policy of shutting out aliens, has systematically remained uncommunicated by the media and the authorities.

*

That the crux of the matter is such a policy, is also abundantly clear from an important and honest report from the Belgian SIRENE office, entitled The Schengen Information System and its Implementation in Belgium (1994).

But the Belgian SIRENE report also shows, most importantly, that *the policy of shutting out aliens is intimately related to the maintenance of public order and State security,* thus corroborating in a very concrete way our earlier reading of the Schengen Convention and other authoritative documents. The two aspects of Schengen are two sides of the same coin: In line with Schengen thinking, aliens currently constitute what is believed to be a primary threat to public order and State security.

The Belgian report explicitly states that the SIS is not a "criminal police service", but a service responsible for the control of all aliens who have been or will be refused entry into the Schengen territory. In more detail: We are told that the SIS "is not meant to replace or imitate Interpol", and that the two are "totally different": While the purpose of Interpol, the report says, is to coordinate

"the combating of crime", the purpose of the SIS is "to guarantee the security within the Schengen countries; thus, all aliens to whom the entry is to be refused are introduced into the S.I.S, ..." (p. 39). The connection between control of aliens and maintenance of public order and security is abundantly clear.

In addition the SIS is, according to the Belgian report, responsible for storing information about persons in general who are supposed to threaten state security: The last quote given above continues as follows: "... as well as persons reported by the State security". Such persons may also be aliens, including aliens who reside in the Schengen countries, but they may of course also be other kinds of "trouble makers".

The secret SIRENE manual mentioned earlier, provides the concrete procedure for storing information about "persons reported by the State security" (Chapter 4.1.2 of the manual). The concrete institutions responsible for State security - in Norway, the secret police - are separate from SIRENE offices. The actual exchange of information takes place between the former institutions. When this exchange is completed, the State security institution wanting to store sensitive information into the SIS, informs its national SIRENE office of the result of the exchange, whereupon the SIRENE office in question may present its objections against including the information. The SIRENE office in question also informs the other national SIRENE offices, which may invoke their rights. When this round is completed in a satisfactory way, the first SIRENE office approves the report, which becomes a part of the information used for "discreet surveillance" pursuant to Article 99.3 of the Schengen Convention (see above).

Norwegian authorities have argued that the procedure summarised here is restrictive. This is true - on paper. Information provided by the Norwegian so-called "Lund Report" of 28 March 1996, in which extensive illegal, politically inspired surveillance for decades and right up to the present was unequivocally documented, goes to show how much restrictive procedures on paper are worth in an area like this. Furthermore, it should be made entirely clear that even if the procedure of storing State security information in the SIS is restrictive, the access to the information which has been stored is not. According to a note from the Steering Committee of the SIS of 17 June 1994, *as many as 34 different police agencies are allowed to request information pursuant to Article 99.3.* Germany is seemingly fairly restrictive: Only one agency is allowed to request information pursuant to Article 99.3. But this agency is Bundeskriminalamt, BKA, which in turn has close contacts with the German intelligence services (Bundesverfassungschutz and Bundesnachrichtendienst). The cooperation inter alia takes place through KGT (Kordinationsgruppe Terrorismusbekämfung). In Greece, Spain and Luxembourg 2 police agencies have access, in France, Italy and Portugal the figure is 4, in the Netherlands there are 5 and in Belgium 10. Briefly put, and to use a Norwegian expression : At the receiving end, the system "leaks like a strainer".

The emphasis on public order and security in a broad sense of the word is also documented concretely in "Draft Schengen Manual on Police Cooperation in Maintaining Public Order and Security", prepared by the Schengen Working Group I on Police and Security 11. June 1997. The draft manual is based on Article 46 in the Schengen Convention - a very wide and open article (see above). On p. 2, the draft manual says (second emphasis mine):

> *Cooperation pursuant to the manual shall apply,* inter alia, *to events where large numbers of persons from more than one country congregate in one or more Schengen States and where the main purpose of the police presence is to maintain public order and security and prevent criminal offences. Examples of these are sports events, rock concerts, demonstrations [!] or road blockades".*

But not only "large numbers of persons" may be involved, because the manual continues as follows (p.2, my emphasis):

> *This cooperation shall not be confined to large-scale events but can also apply to the movement and activities of concentrations of persons, regardless of size, which may pose a threat to public order and security.*

Small groups of people may, in other words, also be scrutinised, on very vague grounds.

The cooperation may involve more than two neighbouring Schengen States, and may be extended through the Schengen realm (p.2, my emphasis):

> *Cooperation shall not be confined to neighbouring Schengen States, but may also take place between Schengen States which do not have a common border and Schengen States of transit.*

A list of "central authorities", to be set up as "liaison points" in each Schengen State, shall supply one another "bidden or unbidden" with information "if circumstances arise or sizeable groups of persons that may pose a threat to public order and security move through or towards other Schengen States" (p. 3). The information shall be supplied at as early a stage as possible. A broad check list of information to be exchanged is presented. Liaison officers can attend and work with the police of other Schengen States, and should the circumstances give cause (p. 5),

> *police authorities of Schengen States concerned may, with a view to coordinating operations, set up joint command and coordination centres.*

In short: While governments and other responsible authorities emphasise the struggle against traditional, serious international crime as Schengen's main goal, all of the empirical and documentary material in hand clearly shows that the goal is to be found at the cross point between the shutting out of aliens and the protection of vaguely defined public order and State security. To repeat, the latter concepts may mean almost whatever you like, and may certainly include politically oriented behaviour. Though non-aliens may be involved, now or in the future, aliens presumably constitute the main threat to public order and State security: The Muslim "threat", for example, represents "a new enemy" after the breakdown of the Soviet Union and the disappearance of "the communist enemy".

This is the reason why Schengen has been called "Fortress Europe". We are reminded of our own historical past.

The above-mentioned Draft Schengen Manual on Police Cooperation in Maintaining Public Order and Security clearly suggests that there is a movement towards a common Schengen operative force with regard to these issues: Police authorities may " set up joint command and coordination centres". The same is indicated in a Declaration of the Executive Committee of 16 September 1998, in which the Central Group in Schengen is instructed "to examine whether the advice and support afforded by the officers of one Contracting State in the framework of external border controls of another Contracting State would improve security at Schengen's external borders", and, "if necessary, to quickly draw up a plan on the reciprocal secondment of liaison officers at the external borders, notably including proposals [inter alia] on ... the exact locations along the external borders to receive assistance in the form of advice and support." In plain English this means that let us say German liaison officers may be placed along the Italian coast to prevent the entry of Kurdish or Albanian refugees, or, similarly, along the long and rather uncontrollable Norwegian coast. Obviously, the next natural step is a joint Schengen border police force, in time and with the implementation of the Amsterdam treaty most likely integrated with the Europol police force which is clearly in the making (see below).

*

The Schengen system has only been in existence for a few years, but we already have concrete examples which either document or show with great probability that the system is being used for downright political purposes. In September 1998 a Greenpeace activist, who had protested against the French atomic bomb tests in 1995 and who had been declared unwanted in France, was refused entry into Holland. She was stopped at the Amsterdam airport, Schipol. On what grounds? On the grounds that she was declared an "unwanted alien" pursuant to Article 96 in the Schengen Convention.[13] Furthermore: At the EU summit in Amsterdam in June 1997 there were political

[13] Source: The Norwegian daily *Dagbladet*, 7. September 1998, verfied by several other sources.

demonstrations. The demonstrations, which according to observers represented no threat to order and security, were met by a great deal of police brutality. According to the police, 609 persons were arrested. Their conditions while in custody were appalling. Actually, more people were taken in custody, inter alia a groups of Italians who were arrested and deported. 29 Danes were arrested and deported to Denmark by a military plane escorted by a fighter plane. The Danish Consul in Amsterdam protested because she was not allowed to visit the Danes who had been taken into custody. Several Swedish citizens were also deported. Later on, the victims of police brutality were awarded damages. In this instance, we cannot document beyond doubt that the Schengen Information System or the SIRENE system were used, or that the demonstrators were registered in these systems for later use. But it is highly probable that registration took place, in view of the fact that the demonstrations were directed towards the EU's central institutions. Observers viewed the police actions which took place - and which involved helicopters, armed vehicles and so on - as a large-scale training manoeuvre for the protection of the EU's powerful institutions.[14]

In Schengen: Data Protection?

The SIRENE offices in the various countries also administer the national SIS databases. As far as the SIRENE goes, there are *no* common data protection regulations (to repeat, the SIRENE is not even mentioned in the Schengen Convention). The absence of a common set of legal rules regulating the SIRENE network has been emphasised as a serious defect by the Joint Supervisory Authority (JSA) concerning data protection in Schengen.[15]

As far as the SIS goes, there are data protection rules specified in the convention. It is presupposed that the contracting parties have taken measures at least on the level following from the Council of Europe Convention on Data Protection of 1981. The specific rules are fairly detailed, and many of them may, for the purposes of this article, be roughly grouped under two headings: Rules concerning *information quality* and rules concerning *application security.*

Rules concerning *information quality* are rules intended to secure the correctness of the information. For example: The reporting contracting party is responsible for the accuracy, up-to-dateness and lawfulness of the inclusion of data (Article 195); only the reporting contracting party may be authorised to amend, supplement, correct or delete data which it has introduced (Article 106.1); if one of the contracting parties which has not made a given report finds an item of data legally or factually inaccurate, it is obliged to advise the reporting party about it, and the reporting party is in turn obliged to look into the matter and, if necessary, correct or delete the item (Article 106.2); any person may have factually inaccurate data relating to him or her corrected or have legally inaccurate data deleted (Article 110); any person has the right to ask the supervisory authority, which is to be established in each country (Article 114.1), to check the data about the person who is included in the SIS, and the use which is made of such data - a right which is governed by national law (Article 114.2); the right of any person to have access to data relating to him or her is to be exercised in accordance with national law (Article 109.1); and so on.

Rules concerning what I here call *application security* are rules intended to secure the proper use of the information. For example: Only specified authorities have access to data included in the SIS, and users may only search data which are necessary for the performance of their tasks (Article 101.1 and 3); personal data for which the convention provides may not be transmitted before specified provisions for the protection of personal data have entered into force in the receiving countries (Article 126.1); the receiving party may use the data only for the purposes for which the convention stipulates (Article 126.3 a); data may not be used for administrative purposes (Article 102.4); and so on.

However, a whole series of decisive problems are attached to rules such as these.

*

[14] Source: Henrik Broberg in Tromsø, Norway; "Written Report from Eye Witnesses of the Demonstrations and the Police Actions" (undated); a *Black Paper* written and distributed on the Internet by eye witnesses.

[15] Source: *Fortress Europe?* December 1996--January 1997, p. 5.

Firstly, a number of the most important rules concerning information quality - the right of citizens to have inaccurate data corrected or deleted, their right to ask the national supervisory authority to check data, and so on - depend entirely on the practical possibility of having access to the data. If people do not have access, the rules are of little help. It should be noted that the convention itself contains very important limitations on such access: Communication of information shall be "refused if it may undermine the performance of the legal task specified in the report or in order to protect the rights and freedoms of others". Furthermore, it "shall be refused in any event during the period of reporting for the purposes of discreet surveillance" (Article 109.2). Equally important is the fact that access to information over and above this is totally dependent on national legislation. In many countries, including Norway, the work registers of the police are as a general rule exempt from access.[16]

Secondly, the application of the rules is to a large extent dependent on police practices in various countries, and it is well known that police practices vary greatly. As the Danish professor of law, Peter Blume, has formulated it: "Such differences in legal culture [are] an Achilles heel of such regulations" (Blume 1992, p. 70). Actual data protection is further decreased by the fact, mentioned above, that there is a total of close to 49,000 access points to the SIS throughout Europe, and by the fact that the usage of the system is far from only limited to the border police: In the above-mentioned note from the Steering Committee of SIS of 17 June 1994, it is reported that a total of 63 institutions responsible for various police functions have access to the SIS pursuant to one or more of the Articles 95-100 (34 of them have access pursuant to the "State security rule" contained in 99.3, see above). Many of the institutions are very large police units (for further details, see Mathiesen 1997 a, p. 47). Political and police authorities regularly emphasise that the inclusion of data in the SIS is restrictive and limited by national legislation. But again, the retrieval of data across the board and in general is certainly not limited as far as the police are concerned. For example, information stored by Denmark in accordance with Danish legislation, may be retrieved in all of the other countries, regardless of differences in legislation, and information stored by all of the other countries according to their legislation, may be retrieved by Denmark regardless of whether the information is stored according to legislation similar to Denmark's.

Thirdly, the common Joint Supervisory Authority, JSA, which has been established to control the SIS in terms of data protection, is a very weak agency, largely lacking practical control possibilities and certainly lacking sanctions. The JSA has two representatives from each country. The director of the Norwegian National Supervisory Authority, Georg Apenes, is one of the Norwegian representatives. He had inter alia the following to say about the JSA at a hearing about Schengen in the Foreign Committee of the Norwegian Parliament 5 May 1997 (translated from the Norwegian by the author):

> *It is a small agency. There are two from each country. They have no sanctions, no secretariat, and as of today they do not even have a phone. A substantial part of the documents which we were supposed to relate to, did not exist in an English translation and not in any of the Nordic languages, so if this is not improved, our possibilities of being an Authority - that is, an authority which is listened to and which is taken seriously by the executive institutions - are probably rather small.*

The problems emphasised by the Norwegian director will hardly disappear if the JSA at long last, is provided with a phone. The JSA issued its first activity report in the Spring of 1997. The report

---

[16] Preparing Schengen for Norway, the Norwegian Parliament has passed an act implementing the Schengen rules concerning the SIS. According to the act, though a police work register, the SIS will not be exempt from general access. But the limitations specified as "musts" in the convention (see above) will of course be upheld, and they are wide and discretionary. It is up to the National Bureau of Criminal Investigation to decide whether an applicant will get access, and the Bureau will function as Norway's national SIRENE-office. In other words, the fox will be set to guard the geese. Complaints will be decided by the Ministry of Justice, not by the Norwegian Data Supervisory Authority, though the latter Authority will function as the National Supervisory Authority of the SIS. Complaints will be submitted to the National Advisory Authority only after the complaint process is over. Correction of information and compensation claimed by persons who do get access will be handled according to the same procedure.

covered the period between March 1995 and March 1997, and confirmed that the JSA does not have any sanctions at its disposal, that its work is often obstructed by various Schengen authorities (the agency had at that time considerable difficulties in getting access to the necessary documents), that its budget is very small, it personnel small[17] and its authority weak. A special problem mentioned by the agency are the so-called "super users" of the SIS: Users who not only have access to any file in the system, but who also may change the files without leaving traces of the search operation. The JSA is worried about the large number of systems of police cooperation which are in the making in Europe (more about this below), and characterises the various sets of data protection rules which exist as a "legal labyrinth".[18]

The criticism continues in JSA's second annual report, covering the period March 1997-March 1998. By way of introduction, the JSA states:

> *When this report was finalised, more than one year after the C.SIS inspection, the JSA still had not received a response to its recommendations from the Schengen decision-making bodies, the only reply to have been received stemming from the French Ministry of the Interior. It was not until February 1998 that the JSA received part of the information on the C.SIS it requires to perform its tasks.*
>
> *Despite the fact that some headway has been made, there still remains a great deal to be done. Although the inspection visit by the JSA to the C.SIS in Strasbourg in 1996 showed that the system on the whole worked well, it also brought to light a number of problems, some of which pose major difficulties as regards integrity.*[19]

---

[17] The 1999 budget proposal for the JSA was 1,050,000 Danish crowns, an increase from 1998. Out of this, 535,000 Danish crowns were earmarked "personel". Compare this with the budget proposal of 44,110,000 Danish crowns for the central SIS database in Strasbourg (in addition, the national SIS bases are paid for by the individual countries). Of the 44,110,000 crowns, 33,470,000 crowns were proposed for establishing *SIS I plus* and *SIS II* (source: Memorandum from the Danish Ministry of Justice to the Legal Committee of Parliament, 4 December 1998). Establishing the new SIS generations will take much more than one year, and continual modernization is expected.

[18] See Activity Report March 1995—March 1997 of the Schengen Supervisory Authority. For a detailed and excellent review of the report, see *Fortress Europe?*, June 1997. Within the context of the action plan on the so-called "common area of freedom, security and justice" (more about this below) ideas about data protection within the third (interstate) pillar of the EU have been debated for several years. A report of 4 February 1999 (5643/99 LIMITE JAI 3; reference documents: Italian initiative, JAI 15, and a resolution by the European Data Protection Commissioners, JAI 16; presented in full text in Statewatch European Monitor Vol. 1, No. 2 1999, pp. 12—14), sets out – as Statewatch summarizes – three distinct areas: 1) the exchange of data between EU member states, 2) "common data collection" (e.g. Europol, Eurodac, SIS), and 3) exchange of data by "other bodies". The report (the Italian initiative) "deplores, against the background of increasingly intense cooperation in the Third Pillar, the fragmentation of data protection provisions for various complex information systems (e.g. SIS, Europol, CIS) ...", and "suggests devising uniform standards which would have to be developed and could then be incorporated into new systems (e.g. EIS) as established elements". This says a lot both about the increasing integration of the information systems, which is openly admitted, and about the problems of regulation. But, as *Statewatch* comments (p. 12), the report "does not address the powers and resources which are essential if supervisory authorities are to be meaningful".

[19] Annual Report March 1997--March 1998 of the Activities of Schengen Joint Supervisory Authority, p. 8. For a comprehensive review of the report, see *Fortress Europe*, August 1998, pp. 12--15. In a declaration attached to the report, the three Nordic data protection commissioners, who are attending JSA meetings pending the countries' full integration in Schengen, noted that "it is of greatest importance that the advice and opinions given [by the JSA] are observed and respected by the central as well as the national bodies in the Schengen system. ... The Nordic observers are of the opinion that the JSA may need to have its economic resources strengthened in the future. They see an immediate need to further strengthen the administrative capacity of the secretariat but will also not exclude the need for more formal authority" (source: *Fortress Europe*, August 1998, p. 12). This is a very strong criticism formulated in bureaucreatic language. *Fortress Europe* commented the declaration in the following words: "More clearly than the Report itself, the Nordic Declaration suggests that the problems, well-described in the JSA's first annual Report, still remain." An important issue confronting the JSA in the report, was the practice of certain member states (including Germany) of keeping supplementary data to the SIS transmitted by other member states through the SIRENE exchange even after the alerts concerned had been deleted in the SIS. In justifying their keeping SIS-related data gathered through the SIRENE exchange for other purposes, the member states invoked the secret SIRENE manual (see above). The JSA demanded an end to the practice as well as a revision of the SIRENE manual on this point. Nothing indicates a quick response to this request from the member states. In an answer to a question from a member of the German *Bundestag*, the German government made it very clear that it has no intention of departing from current practice. Another issue was the practice of making CD-rom copies of the SIS

In the annual report covering March 1998—March 1999, criticism is continued. A telling example of JSA's lack of control of the SIS system was revealed in November/December 1997. Secret documents with sensitive personal information were found at a train station in Belgium. The documents were accessible to everyone who passed by. Sensitive material was also seized in the apartment of a Belgian who had been arrested. The Danish minister of justice, Frank Jensen, characterised what had happened as "a serious breach of security in the SIS". One of the Danish representatives in the JSA called it "monstrous and entirely unacceptable". The then president of the JSA, Alex Turk, was "very worried" over the situation, and looked forward to the December meeting of the JSA, where the leakage would be discussed (all quotes from the Danish newspaper *Information*, 3 December 1997). At that meeting, the JSA

> *expressed its alarm at the incident involving the documents stolen from SIRENE Belgium, which has dramatically demonstrated the need to continuously improve security measures for the SIS (Schengen Information System) and the exchanges of Schengen information.*[20]

To be sure, the incident and the result of the JSA meeting was considered by the Schengen Executive Committee, which "took note of the results of the JSA meeting on 12 December 1997". The incoming Belgian Presidency "made it clear that data protection should be a priority area during its Presidency".[21] No wonder. Bearing in mind how many persons, computers and agencies throughout Europe who have access to the SIS, the Belgian incident represents an uncontrollable and normal kind of event which no doubt will occur again. This time, we were lucky in having the incident publicly exposed.

Fourthly, even the most precise rules are likely to be inadequate in this area in the light of the rapid and enormous development of IT- and other relevant technology. This is well known, and the director of the Norwegian National Supervisory Authority referred to it in the following telling words at the above-mentioned hearing in the Norwegian Parliament (translation as above):

> *But I can perhaps mentioned that at this meeting, which I referred to earlier, people were extremely preoccupied with - and predicted - future distribution of this register [the SIS, TM] on CD-rom, to be used for example by the embassies of the member states which were not directly 'on line' ... due to lack of technical facilities. And in this connection my colleagues, who represented these other countries, were deeply sceptical to having floating round the world CD-rom versions of unknown quality which nobody would know when would be obsolete.*

A plethora of further systems

Schengen does not stand alone.

As I have intimated already, during the 1990s a whole plethora of other proposals, drafts and actual establishments of registration- and surveillance systems has developed in Europe. A *surveillant state* is rapidly becoming a reality. As I have said, at present - but not necessarily in the medium range and long range future - Schengen appears to be a kind of core system in this plethora, which the other systems relate and are drawn to. I shall give four examples.[22] Space does not permit detailed discussion; they are all discussed in much greater detail in a number of issues of *Fortress Europe?* and *Statewatch*, and in Mathiesen 1997a.

(source: *Fortress Europe?* as above).

[20] From a Press Release of the JSA, December 1997.

[21] From Press Release on the Meeting of the Schengen Executive Committee, 15 December 1997.

[22] In addition there are others, such as the CIS, Customs Information System, which is in the making, and which will become a joint European registration system concerning customs. A German initiative seeks to extend the role of the CIS to cover "suspects" (people or companies) who are, or have been in the past, the subject of an investigation (whether or not any evidence was found of unlawful behaviour). Such a development would be very dangerous from the point of view of civil liberties. Source: Statewatch European Monitor Vol 1 No. 2, 1999, pp. 14—15.

Eurodac

The so-called *Dublin Convention* (Convention Determining the State Responsible for Examining Applications for Asylum Lodged in one of the Member States of the European Communities) establishes the principle that a single state is to have the responsibility for handling an application for asylum. The convention contains a series of rules about asylum, and entered into force in a majority of EU states on 1 December 1997 (somewhat later in a minority of states). The Dublin Convention, concentrating on asylum rules, is narrower in scope than the Schengen Convention. Pursuant to a protocol from the Schengen Executive Committee dated 26 April 1994, the Dublin Convention replaced the chapter on asylum in the Schengen Convention as the former convention entered into force. In terms of purposes and aims, with an emphasis on harmonisation of asylum policies, the Dublin Convention strongly resembles the original Schengen rules about asylum. The differences are mostly of a rather technical nature, and not related to substance (see van der Klaauw 1998).[23]

Related to the Dublin Convention there are very concrete plans (in the form of a Convention on Eurodac) of establishing a so-called *Eurodac register*. The Eurodac register is supposed to facilitate the enforcement of the Dublin Convention.[24] Eurodac is designed as a register storing the fingerprints of asylum seekers, but also of other personal data. The register is supposed to be (quotes translated from the Danish version by the author) "a European central register". Forced registration of all asylum seekers over 14 years of age in all EU member states is envisaged. Fingerprints are supposed to be "stored temporarily" in Eurodac's central register "for a period of 10 years". There are only two exceptions from this: The files of persons who have been granted citizenship in a member state are to be deleted, and the files of persons who have been granted status as refugees pursuant to the UN refuge convention are to be barred from general use, and may only be used for statistical purposes. At the earliest five years after the establishment of the central data base, the Council shall consider whether the latter files are to be stored or deleted.

Certain rights to have data corrected or deleted pursuant to national legislation are proposed, but since Eurodac will be a work register for the police, those registered will (like those registered in the SIS, see above) be barred from access to the data in many countries. In order to invoke his or her rights to have information corrected or deleted, the registered person may – again pursuant to national legislation – bring an action before the courts or pursue the issue as a complaint to the competent authorities. But to bring an action before the courts is a very complicated thing in general, and certainly an enormously complicated road for asylum seekers in an uncertain life situation.

The JHA Council reached political agreement ("global agreement") on the contents of the draft convention 3-4 December 1998.[25]

Independently of Schengen's integration in the EU structure (through the Amsterdam treaty, see above), Schengen will be provided with Eurodac: To repeat, the Dublin Convention, which constitutes the basis of Eurodac, has already replaced the Schengen rules about asylum. And there are further clear signs of integration:

Recently it was proposed that the scope of Eurodac be extended to the collection, storage, exchange and comparison of fingerprints of so-called illegal migrants, and not only asylum seekers (van der Klaauw 1998, p.7). In practice, this means the storage etc. of persons who are crossing the EU border without valid documentation - undocumented migrants. Large numbers of undocumented migrants are in practice political refugees from third world countries where visas are necessary in order to enter the EU realm. A detail has concerned the question of whether the extension of

[23] In advance, during an early stage of the country's application for Schengen association, the non-EU country Norway accepted the substitution of the original Schengen asylum rules with the EU Dublin Convention (Norwegian reply of 7 December 1995 to a Schengen questionnaire; for further details, see Mathiesen 1997 a, p. 74). At the time, the social democrats were in power. The acceptance is one of the many examples of the eagerness on the part of the social democrats (along with the right wing parties in Parliament) to integrate Norway as much as possible into the EU, in conflict with the national referendum in 1994 where the majority of the population said "no" to EU membership.

[24] Letter from the German Ministry of the Interior to the Bundestag 1 October 1997, p. 2.

[25] At the General Affairs Council on 7-8 December 1998 a so-called High Level Group on Asylum and Migration was created, connected to an Austrian migration strategy paper. Source: *Statewatch* November--December 1998, p. 22.

Eurodac to so-called illegal migrants should be included in the Convention or in a protocol attached to the Convention. At the JHA Council meeting 19 March 1998, a majority of Member States preferred the protocol solution, fearing that an amendment of the draft Convention would cause delay. Germany, Austria and the Netherlands argued for an immediate amendment of the draft Convention. In any case, the Council reached agreement on the principle of widening the scope of Eurodac.[26] According to the minutes from the JHA Council meeting 24 September 1998, agreement was reached on the protocol alternative. There was some disagreement over the period of storage of the fingerprints of so-called illegal immigrants, and at the latter JHA Council meeting the Presidency "proposed to pursue work on the basis of a duration of 2 years, which would be a compromise ...".

The draft protocol was up for discussion at the JHA Council meeting 3-4 December 1998, but postponed with a view towards further political preparation. Agreement was reached at the JHA Council meeting in March 1999. In view of the entry into force of the Amsterdam Treaty on 1 May 1999, the Council presupposed that the EU Commission would prepare a common instrument to supplant the convention as well as the protocol, with a view towards final agreement by the end of 1999.

The history of the issue of fingerprinting "illegal migrants" shows how Schengen and Eurodac concerns are intertwined. The issue was, notably, raised in a decision by the Schengen Executive Committee on 15 December 1997, which advocated the "taking of fingerprints of each illegal third country national immigrant whose identity cannot be established beyond doubt ... and storing of the data for information exchange with other authorities of the member states".[27] The decision on fingerprinting was a part of a larger Schengen action plan effecting, "without delay", a whole string of specific measures against so-called illegal immigration.[28] The electronic exchange of finger prints is possible via the SIRENE-network.[29], and the proposed fingerprinting would, as *Statewatch* comments (January-February 1998, p. 1),

> *create a major source of information to be entered into the EU's EURODAC computerised fingerprint database when it comes on line...*

The issue of fingerprinting "illegal migrants" was again raised, now with direct reference to Eurodac, in a 46-point EU Action Plan of 26 January 1998, designed to curb the entry into the EU of "illegal refugees".[30] As *Fortress Europe?* observes (January-February 1998, p. 1), the background of the rushed EU Action Plan was the arrival in Italy, right before and on New Year's Day 1998, "of two boat-loads of forced migrants, many of them Kurds from Turkey and Northern Iraq. ... [T]he arrival of less than 2,000 undocumented forced migrants [was] used as a welcome pretext for clamping down on refugees, further tightening border controls and promoting extended police cooperation and police powers".[31] *Statewatch* comments (January-February 1998, p. 3) that the EU Action Plan:

---

[26] Source: *Fortress Europe?* May 1998.

[27] Source: *Statewatch* January--February 1998, p. 1.

[28] Source: *Fortress Europe?* January--February 1998, pp. 3--4. *Fortress Europe?* observes that less than a month after the meeting of the Schengen Executive Committee, on 8 January 1998, a secretive police meeting took place in Rome, where "police chiefs from the six Schengen countries most concerned by illegal immigration met ... with the Turkish police chief to discuss practical cooperation in the fight against 'illegal immigration' ...".

[29] Source: *Fortress Europe?* January--February 1998, p. 3.

[30] Sources: *Fortress Europe?* January--February 1998, pp. 1--3; *Statewatch* January--February 1998, pp. 3--4. In March 1998 a high level EU delegation visited Turkey (Istanbul and Ankara), with a view towards closer cooperation with Turkey regarding the screening of asylum-seekers, detection of false documents, detaining illegal immigrants, etc.; source: *Statewatch* May--August 1998, p. 1--2. Within the EU, a number of intiatives have been taken to curb "illegal immigration"; for more details, see Statewatch European Monitor Vol 1 No. 2, 1999. The initiatives clearly show how Schengen fits neatly into the EU attempts to control external borders.

[31] From a Schengen point of view, Italy is a kind of "Trojan Horse" among the member states: Italian legislation apparently implies that refugees who are unable to identify themselves are allowed to remain in the country for a short period of time, and may consequently disappear. In 1998 this was the basis of a heated debate, especially in connection with North African refugees to Sicily.

thus follows in the wake of the Schengen Executive Committee of 15 December 1997.

Formally, the Schengen's moves to establish a fingerprint system are bilateral, and independent of Eurodac. But, as with so many other aspects of the Schengen development, the informal contacts and understandings are decisive, in addition to the fact that the people taking part in meetings and the making of plans inside and outside Schengen are to a large extent the same. In practice, then, the integration of Schengen concerns with the coming Eurodac system is quite obvious, and the separation between the two utterly artificial. The pending integration of Schengen in the EU structure will complete the process of fusion of today's Schengen and Eurodac.

Let me add that as a parallel to Eurodac, a work group in the EU has been developing a European central computerised system, within the General Secretariat of the JHA Council, for the storage and exchange of pictures. The system is called FADO (False and Authentic Documents). The purpose is swift electronic exchange concerning authentic and false documents. As a memo from the Danish Ministry of the Interior stated the matter in December 1998 (p. 28): "The system will be based on Internet technology and may be used by a central data base in each member state through a secure Internet connection. In Denmark, the National Police will have that competence". Internet technology may, in other words, be used for many purposes. A joint action for the setting up of FADO was adopted without discussion at the JHA Council meeting 3-4 December 1998.

Several countries, including Norway, have already established systems for national registration of fingerprints of asylum seekers. A widening of the national systems to include all "illegal migrants" will, of course, be technically simple. The countries are, in other words, prepared for Eurodac. It has been documented that the Danish National Police (Rigspolitiet) has been exchanging fingerprints of asylum seekers with a number of EU states ever since the Dublin Convention entered into force on 1 September 1997, and despite the fact that the Eurodac Convention is not yet signed.[32] A network of fingerprint databases covering Norway, Denmark, Sweden and Finland is being set up by the American company Printrack International.[33] As *Statewatch* observes (July-October 1997, p. 2), Printrack "supplies biometric identification systems used primarily in law enforcement applications such as welfare and immigration control. It [also] provides networked fingerprint, photo imaging and automated records management systems ..." A Joint Control Authority (JCA) is going to monitor the processing of data in Eurodac, and check the lawfulness of transmissions.[34] But while it will have rights to "control" and "examine", as well as make "suggestions for improvement", it will, as *Fortress Europe?* points out (January-February 1998, p. 7),

> *have no powers to sanction practices in breach of the Convention or of international obligations with respect to the protection and security of personal data. In view of the problems encountered by the corresponding Schengen body in carrying out its tasks ... it is also doubtful whether the JCA, with only two representatives per member state, will be in a position to ensure effective control.*

Eurodac as a "European central register" is so far without precedent in European history. It will imply long-term or permanent registration and surveillance of (and throw lasting suspicion on) large population groups throughout Europe.

*

The control of asylum seekers and political migrants through Schengen and Eurodac is given added support by a so-called "Strategy Paper on Asylum and Immigration", leaked from the Austrian EU Presidency in early September 1998. The strategy paper proposes the development of a self-contained migration and asylum strategy at a European level with a view towards establishing the key elements of effective migration management and enhancing the EU's ability to act in this respect. The

[32] Source: *Fortress Europe?* May 1998.
[33] Source: *Statewatch* July--October 1997.
[34] Source: *Fortress Europe?* January--February 1998.

background is deep dissatisfaction with various holes in EU asylum and migration control, and has been heavily criticised by human rights organisations.[35] Schengen and Eurodac fit nicely into the strategy outlined. The paper was up for discussion at the JHA Council meeting 3-4 December 1998, and considered "a useful contribution to the work of the cross-pillar Task Force proposed by the Dutch delegation and will also serve in preparing the special Justice and Home Affairs European Council in Tampere in October 1999".[36] The numerous EU activities geared towards asylum and migration control interlock.

EIS

The so-called *Border Control Convention*, which has been finalised in negotiations between the EU member states, aims at effective control of persons along the EU's common exterior border.

Related to the Border Control Convention, work has been going on to establish a comprehensive information system, the so-called *European Information System*, EIS, designed to contain the necessary information. As we have already seen, the draft of the EIS convention explicitly mentions the SIRENE system, which is already developing fast in Schengen.

On 27 June 1994, the Schengen Executive Committee stated that "[o]nly one information system [should] be used in Europe for the registration and persons and objects in connection with border controls, verifications and other police controls". The committee furthermore stated that provided the EIS Convention was enforced, Schengen would be "ready" to place the SIS at the disposal of the EU member states outside Schengen. In other words, as early as in 1994 a fusion between the two systems was being planned.

With the Amsterdam Treaty of 1997, which integrates the Schengen measures into the EU structure, SIS will take over the intended functions of EIS, and in fact be renamed EIS.

Europol

The convention which lies at the basis of Europol, with the *Europol Computer Systems*, TECS, is ratified by all EU states. The last state to do so was Belgium - in June 1998. The convention entered into force on 1 October 1998 and Europol became operational on 1 July 1999. Europol is a joint police unit within the EU, originally - before ratification - established as a Europol drugs unit (EDU), but with an enormous potential for development. In contrast to Schengen, Europol aims at serious international crime. At the same time, the data protection problems and other issues are formidable.

As a *Statewatch* publication has put it (Bunyan 1995, p. 2),

> *Europol is one of a number of inter-linking EU-wide computer data bases being set up which, once created, will potentially impinge on the rights of a whole range of people for the foreseeable future.*

The Europol Computer Systems will have three main subsystems.

Firstly, there is a *central information system* (Article 8 in the Europol Convention). Information may be entered about persons who by national law are suspected of having committed or of having taken part in criminal offences under Europol's competence, or persons about whom there are serious grounds, under national law, to believe will commit such offences (Articles 8.1.1 and 8.1.2). In other words, the system is clearly geared not only towards persons suspected of having committed any of the offences in question, but towards persons suspected of participation in a wider sense of the word as well as towards a broad category of possible future criminals and possible future offences - certainly, a very extensive and diffuse category.

What kinds of information may be included in the central information system? The system may be used to store, modify and utilise (Article 8.2) certain standardised personal data (name,

[35] Source: *Fortress Europe?* December 1998, pp. 1—4.
[36] Source: Report from the JHA Council meeting, taken from the Internet.

aliases, date and place of birth, nationality and sex), and, "where necessary, other characteristics likely to assist in identification, including any specific objective physical characteristics not subject to change". The most obvious other "objective physical characteristic" is a person's race. In addition (Article 8.3), certain "details concerning the persons referred to" may be included: "criminal offences [and] alleged crimes", "means which were or may be used to commit the crimes", "departments handling the case and their filing references", "suspected membership of a criminal organisation" and relevant convictions. The latter data may also be included "when they do not yet contain any reference to persons". For example, "alleged crimes" may be included without reference to any person.

Also (Article 8.4), "[a]dditional information held by Europol or national units concerning the groups or persons referred to in paragraph 1 may be communicated to any national unit or Europol should either so request. National units shall do so in compliance with their national law". In short, from Articles 8.2 through to Article 8.4 the information which may be included/communicated is continuously widened, ending with the catch-all "[a]dditional information".

*

Secondly, there are the *work files for the purposes of analysis* (Article 10 in the Europol Convention). These are special, temporary work files set up for the analysis of specific areas of activity. The work files may contain extensive personal data, not only (Article 10.1 No. 1) about persons registered in the central information system pursuant to Article 8.1, but also (Article 10.1 No. 2-5) about:

- possible witnesses ("persons who might be called on to testify"),
- victims or persons whom there is reason to believe could be victims ("...with regard to whom certain facts give reason for believing that they could be victims..."),
- "contacts and associates", and
- informants ("persons who can provide information on the criminal offences under consideration")

In short, a very wide circle of individuals loosely tied to persons who have been sentenced or are under suspicion.

Thirdly, there is *an index system*, designed in such a way that it is possible to determine whether or not a given item of information is stored.

Let us look more closely at the second of these levels, *the work files*. The kinds of personal information which may be stored in the work files are not specified in the convention, only in so-called "implementation rules", given pursuant to the convention. The implementation rules are not to be approved by parliaments, only unanimously by the Council (Europol Convention, Article 10.1). There is full agreement on the final proposal for implementation rules in the JHA Council (according to minutes from the JHA Council meeting 24 September 1998). The rules were approved by the Europol Management Board in October 1998.

As an example of the kinds of personal information which the work files are designed for, mention should be made of a proposal presented in 1996 concerning supplementary information of a highly personal and intimate kind (doc. 4038/96, my emphasis):

> *It shall be forbidden to collect personal data solely on the grounds that they relate to racial origin, religious or other beliefs, sexual life, political opinions or membership of movements or organisations that are not prohibited by law. Such data may be collected, stored and processed only if they supplement other personal data stored in the analysis file and only where they are absolutely necessary, taking into account the purpose of the file in question.*

The important word here is "solely". It will be seen that the proposal in fact *opens* for inclusion of data about "racial origin, religious or other beliefs, sexual life, political opinions or membership of movements or organisations that are not prohibited by law".

Later, the proposal went through various new editions, inter alia following from criticism by

the European Parliament. But the adopted proposal (OJ C 26, 30.1.99) still opens for the inclusion of such intimate personal data. Article 5.2, first subsection, of the implementation rules applicable to analysis files states:

> *Europol shall also specify in this order whether data relating to racial origin, religious or other beliefs, political opinions, sexual life or health may be included in the analysis work file under the categories mentioned in article 6 [about Article 6 in the implementation rules applicable to analysis files, see below], and why such data are considered to be absolutely necessary for the purpose of the analysis work file concerned.*

Pursuant to the same Article 5.2. second subsection, it appears that with regard to victims, possible victims, possible witnesses and informants, such data can only be included after special grounds are given and upon the explicit request from two or more member states. In practice, these limitations are not particularly strict. For other categories of persons, no such limitations are given.

But what about the European Convention on Data Protection of 1981, and the EU data protection directive 95/46EF? Do they not bar registration of such data? Article 6 of the Council of Europe Convention states that such data "may not be processed automatically unless domestic law provides appropriate safeguards". Clearly, if what is considered "appropriate safeguards" are provided, the data may in fact be processed. Article 3.2 of the EU directive explicitly exempts the directive inter alia from being applicable to "the activities of the State in areas of criminal law". Inclusion of the sensitive information mentioned here in other words falls outside the jurisdiction of the directive.

The final proposal for implementation rules applicable to work files (doc. 6100/4/97) allows (in Article 6) the processing of 53 (!) types of personal data about persons registered in the central information system. The 53 types of personal information are grouped in ten categories, for example "personal details" (fourteen types of data), "physical appearance" (two types of data), "identification means" (five types of data; including forensic information such as fingerprints and DNA evaluation results, though "without information characterising personality"), occupation and related qualifications (five types of data), "economic and financial information" (eight types of data), "behavioural data" (eight types of data; including "life style (such as living above means) and routine", "danger rating" and "criminal related traits and profiles"), and so on.

One of the other categories is named "references to other databases in which information on the person is stored", including Europol, police/customs agencies, other enforcement agencies, international organisations (!), public bodies (!) and private bodies (!).

To reiterate, the above-mentioned types of data may not only be included about persons registered in the central information system, but also about possible witnesses, victims or persons whom there is reason to believe could be victims, contacts and associates, and informants.

The ratification of the Europol Convention took place despite strong criticism from various quarters. Thus, the German supervisory data protection authorities on the federal state level have strongly criticised Europol on the grounds of lacking appropriate security measures. The criticism was levelled at a meeting of federal state supervisory authorities in Bamberg in October 1997.[37] Likewise, the German Association of Judges and the German Director of Public Prosecutions have been critical.[38] To be sure, a joint supervisory body will be established pursuant to Article 24 in the Europol Convention, and a set of "Draft Rules of Procedure of Joint Supervisory Body" was first proposed in late 1997 (doc. 11330/97, 13 October 1997). However, the draft rules largely contained stipulations concerning the formal organisation of the supervisory body: Rules of procedure of the body (membership, chair, working method, and so on), general rules of procedure of the appeals committee (membership, independence and impartiality of members, chair, languages, and so on), and certain specific rules of procedure of the appeals committee. Clearly, real power on the part of the Supervisory Body was not a part of the plan. The same is evident from the draft rules of procedure for the Joint Supervisory Body considered by the JHA Council 24 September 1998, and

[37] Source: *Frankfurter Rundschau*, 25 October 1997.

[38] Source: Personal communication from the editor of *Fortress Europe?*, Nicholas Busch, 3 November 1997.

again by the Council 3-4 December 1998. In the minutes from the latter meeting, taken from the Internet, vague terms like "reviewing" the activities of Europol to ensure that the rights of the individual are not violated and "monitoring" the permissibility of the transmission of data originating from Europol are used. The minutes also show how meetings in the JHA Council (and the EU in general) are conducted to obtain unanimity: The text drawn up proposed an organ which would be neither a court nor purely an administrative body. The Presidency proposed to accept this "and to address the concerns of one delegation by a declaration setting out the conditions for public hearings (generally procedures will be in writing)". The Council "broadly supported the approach of the Presidency" and mandated the competent bodies to finalise the declaration "in view of the rapid adoption of the text on the rules of procedures". Rare "public hearings" will hardly change matters much and hardly give the Supervisory Body more or less say, but pressure to reach unanimity and get Europol quickly on line was great, and the proposal was accepted as a way out and, most likely, a way to save face.

Even those employed within the Europol system as it exists today, admit to problems. Thus, the assistant coordinator in Europol Drugs Unit or EDU (which will be dismantled as Europol proper gets on line) W. Bruggeman, who places great emphasis on regulations such as constitutional guarantees, the Council of Europe Convention on Data Protection, and Recommendation No. R (87) 15 Regulating the Use of Personal Data in the Police Sector, has this to say about the problems:

> *The provisions on data protection are comprehensive in theory, but fatally undermined by the difficulty that is likely to arise in enforcing them. Within the Union, the system will depend crucially on the degree of respect for data protection and individual rights imbued in every police officer involved. This will require not only rigorous training but in many cases a radical change in the culture of the national force concerned. ... When this is added to the feeling among some police officers (both here and abroad) that the ends may justify the means where catching criminals is concerned, the potential danger is apparent* (Bruggeman 1998, p. 48).

Considering that they come from a top level officer in Europol, these are strong words. So are the following words about the linkages out of the EU, to third countries:

> *Europol may transmit personal data to non-EU States if they have 'an adequate level of data protection'. This is left undefined, and ... [t]he pressure to exchange data with such countries in the interests of mutual assistance might well in practice outweigh considerations of strict data protection* (Bruggeman, same source).

*

A protocol attached to the Europol Convention, pursuant to Article 41.1 of the convention, proposes diplomatic immunity for Europol officers within the EU countries. Article 8 of the protocol grants all Europol staff "immunity from the legal process of any kind in respect of words spoken or written, and of acts performed by them, in the exercise of their official functions". Article 12 places on the Europol director a duty to waive immunity "in cases where the immunity would impede the course of justice and can be waived without prejudice to the interests of Europol".[39] To use a Norwegian proverb, this duty amounts to "letting the goat guard the wheat".

On the background of the protocol, the immunity of Europol staff may be extended to third countries: Article 42 of the Europol Convention regulates Europol's relations "with third states and third bodies". Based on this article, a report covering draft rules regarding the external relations of Europol was adopted by the JHA Council on 4 December 1997. Article 7 of that report says that "[a]n agreement reached with a third country may provide for the privileges and immunities which may be necessary for Europol as well as for personnel and liaison officers sent out by Europol".[40] As *Statewatch* comments: "The contentious 'immunities of Europol officers' with the EU could thus be

[39] Quotes taken from *Statewatch* November--December 1997, p. 30.
[40] Quotes taken from *Statewatch*, as above.

extended anywhere in the world".

The protocol on privileges and immunities has been ratified by all EU states. With the convention as well as the protocol ratified and agreement on the rules of procedure for the Joint Supervisory Body, Europol became operational on 1 July 1999.

It may be added that the Amsterdam Treaty contains a rule (Article 30 in revised TEU) extending, as *Statewatch* puts it, Europol's role "from gathering and analysing information and intelligence to setting up investigations, taking part in operations, and possibly simply leaving the arrests to the police of a member state."

The system is planned with a view towards far-reaching integration inter alia with the Schengen Information System. For one thing, article 10.4 No. 1-3 in the Europol Convention establishes a whole range of authorities and bodies within the EU from whom Europol may request information: The European Communities and bodies within them governed by public law, other bodies governed by public law established in the framework of the EU and bodies based on an agreement between two or more Member States within the EU (also, article 10.4. No. 5-7 establishes that information may be requested from international organisations and subordinate bodies governed by public law, other bodies governed by public law based on an agreement between two or more States, and Interpol). Clearly, this opens for integration with the Schengen Information System. In a secret proposal of 9 April 1997 the so-called High Level Group on Organised Crime explicitly recommended, in line with this, that *Europol is given access to the information stored in the Schengen Information System.*[41] This and other recommendations were on the agenda of the Justice and Home Affairs' council meeting 3—4 December 1998 in connection with the action plan on establishing an area of freedom, security and justice, and were also discussed in a report of 26 February 1999 (6245/99 Europol 7). The report inter alia discussed the issue of whether Europol's authority should be extended to actual searches in the SIS[42] (pursuant to the Europol Convention Article 3 (1) point 2 Europol has the task to obtain, collate and analyse information and intelligence, but no authority to search). Furthermore, concrete work directed towards facilitating and easing compatibility between the two systems has been going on for a long time. In a lengthy paper, the then Norwegian liaison officer in Interpol, Iver Frigaard, has outlined a number of the issues, problems and possible solutions (Frigaard 1996). Frigaard sees Europol, Schengen and Interpol as three "mutually interlocking" and "overlapping" policing initiatives. He discusses their relationship on a systems level and on the level of exchange of information in concrete cases. On the systems level he points to the fact that so far (1996) "only" 10 of the 45 states linked to Interpol's information system are also linked to Schengen and Europol. The number of states linking up to all three systems should and may, in his opinion, be increased. In connection with the exchange of information in concrete cases, he points to a lack of harmonisation of the various data systems, and discusses the great need for compatibility between them as well as how it may be attained technologically. The vigorous tenor of the paper clearly suggests that this is a matter of high priority.

Once more, such access and integrative cooperation will be greatly facilitated when the Amsterdam Treaty is enforced. It may be added that at its meeting on 19 March 1998, the JHA Council agreed, without debate and as an "A" point, on rules allowing Europol to request and accept information from non-EU sources (pursuant to Article 10.4. No. 4 of the Europol Convention). The report covers the receipt of data from "third States and third bodies" (a relevant country is Turkey), and includes only the most minimal safeguards on data protection. Thus, assessment of the source and of the information is normally left to the third State or the third body in question. When this self-assessment is not provided, Europol itself shall attempt "as far as possible" to assess "the reliability of the source of information on the basis of the information already in its possession". There are provisions for Europol to delete information, but where a third State or body tells Europol that the information has been corrected or deleted, Europol is not obliged to do likewise inter alia if it has further need to process the information for the purpose of the analysis file.[43] The planned

[41] Source: Original personal communication from the editor of *Fortress Europe?*, Nicholas Busch; see doc. 7421/97 JAI 14.
[42] Source: Statewatch European Monitor Vol 1 No. 2, 1999, pp. 14—17.
[43] Source: *Statewatch* March--April 1998, pp. 24-25; quotes from the rules.

rules are to be supplemented by a series of "memorandums of understanding" between Europol and the central services of each of the non-EU states with whom data are to be exchanged. In short, as *Statewatch* puts in, "Europol prepares for 'global' exchange of data".[44]

Surveillance of telecommunications

The fourth example of the plethora of surveillance systems concerns international cooperation regarding surveillance of telecommunications. There are two systems, the Echelon system serving the "military-intelligence community" (see later) and a new system being put in place for the "law enforcement community". This latter system, which will place phone-calls, e-mails and faxes under surveillance, has acquired a number of different names - here I use the EU-FBI telecommunications surveillance system (or the "EU-FBI system" in short).[45]

In November 1995 a *Memorandum of Understanding on the lawful interception of telecommunications* was signed by the EU countries. The memorandum emphasises that law enforcement ("combating serious crime and protecting national security") requires such interception. The memorandum refers in general terms to "law enforcement agencies", without any clear delimitation: A "law enforcement agency" is defined as a "service authorised by law to carry out telecommunications interceptions". Subsection 2 of the Requirements states:

> *Law enforcement agencies require a real-time, fulltime monitoring capability for the interception of telecommunications. Call associated data should also be provided in real-time. If call associated data cannot be made available in real time, law enforcement agencies require the data to be available as soon as possible upon call termination.*

To be sure, subsection 5 requires "the interception to be designed and implemented to preclude unauthorised or improper use and to safeguard the information related to the interception". The formulation is, however, completely vague, without any specification of how the information is to be safeguarded. Furthermore, the memorandum requires "network operators/service providers to protect information on which and how many interceptions are being or have been performed, and not disclose information on how interceptions are carried out".

As indicated, the memorandum is a EU document. The Schengen convention contains no provision for the interception of telecommunications. I have, however, documented earlier that the SIRENEs already store information obtained through the interception of mobile phones (see the statement made by the director of the Portuguese SIRENE office quoted above). With the integration of Schengen in the EU structure through the Amsterdam Treaty, cross-boundary interception may easily be expanded with the memorandum as a legal source and basis. There will no longer be a separation between EU agreements and Schengen agreements.

A closer look at the background of the memorandum shows how various police systems in the world cooperate and interlock. In 1993, the American FBI held an international conference on law enforcement and advanced telecommunications at the FBI Academy in Quantico, Virginia. Eleven countries inside and outside the EU were represented. Since then this group of states has been working to standardise the requirements for interception on the part of law enforcement agencies. This meeting in Quantico established the so-called "International Law Enforcement Seminar", ILETS, which has operated as an "unseen", secret, group of officials in the area of interception. The group was gradually enlarged, by 1995 counting 20 countries: The 15 EU countries and the US, Canada, Hong Kong, Australia and New Zealand. A document was produced by the group with the aim of establishing a collection of international requirements concerning interception, to be used in the development of national legislation. The document was finalised at a conference in Bonn during the summer of 1994. It emphasised the requirements which law enforcement agencies throughout the

---

[44] Source: *Statewatch* September--October 1998, pp. 20-21.

[45] The "EU-FBI system" has been variously termed: the "Quantico group", the "Group of 20", "ENFOPOL" and ILETS.

world must have satisfied in order to implement interception of telecommunications efficiently.

The EU based its attempts at finding solutions for legal interception on the specifications of requirements formulated with by the FBI and developed by ILETS. The attempts resulted in the above-mentioned EU memorandum, and in November 1995 countries outside the EU were invited to sign it and Norway signed the memorandum straightaway on 23 November 1995. In other words, for the non-EU country Norway, the road to the EU-memorandum went through membership of the ILETS Group.[46] Currently, the memorandum is being updated within the EU.[47]

In short, through the Quantico meeting, an American FBI initiative, and the later ILETS meetings the EU have interacted in paving the way for a global system of surveillance of telecommunications, the EU-FBI system. *Statewatch* (May-June 1997, p1-2) comments on the significance of the memorandum in the following words:

> *[W]ith agreement to cooperate on the basis of the "Memorandum" the group of "20" can work together to ensure that the major providers of the new satellite-based telecommunications systems adhere to the "Requirements" - in effect to ensure compliance by multinational companies.*
>
> *The new era of satellite-based telecommunications will see just four companies -- Iridium, Globalstar, Odyssey and ICO - controlling the "global network of mutually co-operating satellites". In the EU it is expected that there will be only 3 or 4 "ground stations" linked to these systems -- "in France and Italy and perhaps Finland, the UK and Germany".*

A new EU Draft Convention on Mutual Legal Assistance in Criminal Matters will inter alia legitimise such surveillance. The draft convention does not at all limit the powers to intercept telecommunications to any clear conception of "serious crimes". The limits are those set out in the 1959 European Convention on Mutual Assistance in Criminal Matters, which deals with any punishable offence however minor.[48] Neither does the draft convention leave any doubt that the results of interceptions are to be communicated between countries, in a bilateral or multilateral, cross-boundary fashion. For example,[49] Article 6.2 of the Draft Convention as it was formulated in 1997 says that an "order" from a competent authority of the "requesting Member State" can ask for either:

> *the interception, recording and transcription of intercepted correspondence or for interception and direct transmission of intercepted correspondence to the requesting Member State for monitoring and for recording and transcription there.*

As *Statewatch* (May-June 1997) observes:

> *In plain language the results of an interception are either sent ex-post to the 'requesting' member state or, if the member state asks, the interception is transmitted real time (as it is happening) to the "requesting" member state".*

Referring to Article 6.2, a-c, *Fortress Europe* (May 1998, p. 4) comments:

> *The rules are worded so as to enable the interception without interruption in the whole territory of the EU, even of persons, quickly moving between different Member States and using any type of fixed or mobile telecommunication devices and structures.*

---

[46] Source: The Norwegian Aukrust Report 1996. The Aukrust Report refers to the "Quantico Group" rather than ILETS, but more recently (1999) Norwegian authorities have admitted that Norway is a member of ILETS.

[47] Source: Reuters Newswire 3 December 1998.

[48] Pointed out by *Statewatch*, November-December 1998, p. 21.

[49] Source: *Statewatch* May-June 1997, p. 16. See, likewise, *Fortress Europe?* (May 1998), which deals with a series of other aspects of the Draft Convention on Mutual assistance in Criminal Matters, and which presents an interesting systematic comparison between that draft convention and the so-called "Naples II" Convention on Mutual Assistance and Cooperation between Customs Administrations. I return to this comparison below.

Like the EU memorandum of understanding on surveillance of telecommunications, the EU convention on mutual legal assistance will legitimise such surveillance for Schengen once Schengen activities are integrated in the EU structure.

*

Currently, bodies within the EU structure are working to extend the telecommunications plans to the Internet (e-mail) and to new generation satellite mobile phones.

The plans are made within the EU Police Cooperation Working Party (which reports to the Article 36 Committee - the renamed K4 Committee - and the Justice and Home Affairs Council). Its work is highly secret, and it is very hard to get hold of documents.

The existence of the EU-FBI system first came to international attention when *Statewatch* published a report in February 1997.[50] In 1998 the journal *Telepolis* revealed that the system was to be extended to the internet.[51] It showed plans are in the making for monitoring any and all kinds of telecommunication - data, whether encrypted or in clear form, mobile telephony, the new Iridium system and other satellite mobile phone services. Says Armin Medosch (*Telepolis* 30 November 1998 (www as above) it:

> *is aiming at the central terrestrial masterstation of Iridium in Italy as an ideal spot to monitor telecommunications traffic. But also large clearing houses which handle international phone call billing for the big national operators are mentioned as potential sources for the kind of information European police forces are interested in.*

At the moment, the EU-FBI system is not a reality, but a set of proposals drawn up by this working group for police cooperation. Also, the proposals have been heavily criticised, inter alia by Internet suppliers who - as far as the Internet goes - find them problematic in principle and extremely costly (Campbell 1998). After the official documents (with the acronym "ENFOPOL") were leaked, criticism has also been voiced in the EU Parliament, by Irish representative Patricia McKenna (who received very evasive replies). But the plans do show quite clearly the direction of thinking concerning police cooperation, and discussions of the matter have commenced in the JHA Council (for example in the JHA Council meeting in May 1999).

Are, then, plans of this kind technically feasible? The so-called *Echelon* system, which *is* a reality, shows that they are.

*

A parallel surveillance network, partly overlapping with the EU-FBI system in terms of membership states, is called the *Echelon* system. Unlike many of the electronic surveillance systems developed during the cold war, *Echelon* is designed just as much for non-military targets -- governments, organisations and businesses throughout the world. The US, Britain, Canada, New Zealand and Australia are the main participants, with the US as senior partner. A report to the European Parliament by Steve Wright dated 6 January 1998[52] describes the activities of *Echelon* in the following words which, in terms of the technology described, is also relevant to the *EU-FBI system* (pp. 18-19):

---

[50] Source: see http://www.statewatch.org/news2.htm. The 1993-meeting in Quantico initiated by the FBI, and subsequent developments up to and including the EU memorandum in 1995, were described in the above-mentioned Norwegian Aukrust Report, authored by a committee appointed by the Norwegian Ministry of Justice (1996). With this as a main source, an account of these early developments in the EU-FBI system were given in Mathiesen 1997 a.

[51] Source: http://www.telepolis.de/tp/deutsch/special/enfo6329/1.html.

[52] Steve Wright: An Appraisal of Technologies of Political Control, PE 166.499. Revised September 1998.

A wide range of bugging and tapping devices have been evolved to record conversations and to intercept telecommunications traffic. ... However, planting illegal bugs ... is yesterday's technology. ... [T]hese bugs and taps pale into insignificance next to the national and international state run interception networks. ... Modern technology is virtually transparent to the advanced interceptions equipment which can be used to listen in. ... Within Europe, all email, telephone and fax communications are routinely intercepted by the United States National Security Agency,[53] *transferring all target information from the European mainland via the strategic hub of London then by Satellite to Fort Meade in Maryland via the crucial hub in Menwith Hill in the North Yorkshire Moors of the UK. ... The ECHELON system works by indiscriminately intercepting very large quantities of communications and then siphoning out what is valuable using artificial intelligence aids like Memox to find key words. Five nations share the results. ... Each of the five centres supply "dictionaries" to the other four of key words. Phrases, people and places to "tag" and the tagged intercept is forwarded straight to the requesting country. ...*

In a revision of the report, dated September 1998, Wright reports a number of instances where Echelon allegedly has benefited US companies, ranging from arms deals to disputes over car parts. He writes: "If even half of these allegations are true then the European Parliament must act to ensure that such powerful surveillance systems operate to a more democratic consensus".

Echelon's technology is geared towards the interception of telecommunications via satellite. A substantial part of telecommunications today is transported via submarine cables across the oceans. Submarine cables are more difficult to intercept (though easy to intercept as they enter into or come up from the ocean). But the future is with the satellites. On 1 November 1998 the world's first mobile telephone network covering the globe as a whole was opened (and called the world's first "virtual nation" by its promoters). The network is named "Iridium". The network, based on sixty six satellites, enables you to have total and direct coverage through the "country code" 8816. Prices

[53] The US National Security Agency, NSA, was established in 1952 by president Harry Truman. This powerful agency plans, coordinate and executes signal intelligence as well as tasks concerning information security. It is concerned with non-defence as well as defence issues. A main point is to break through and understand foreign communications while at the same time protecting the nation's own communication systems. In this double task lies NSA's main goal and competence. NSA is the world's leading cryptological organisation.

It is Steve Wright's point that the NSA is deeply involved in Echelon. The NSA is an active agency indeed. In July 1999 The New York Times revealed that the NSA had developed a plan for massive electronic surveillance. The plan, entitled *The National Plan for Information Systems Protection*, was presumably directed towards protecting US datasystems against hackers, data terrorists and enemy states, in other words, information security. The plan, however, included strategies to establish a large scale domestic and international Internet monitoring system, to be used by the FBI. One of the plan's proposals called for the creation of a Federal Intrusion Detection Network, FIDNET, to monitor all network activity involving civilian government departments and agencies. FIDNET was to be linked to a similar system in the Defense Department known as the Joint Task Force-Computer Network Defense (JTF-CND) that monitors all Defense Department networks. Both of them were in turn to be linked to private sector Information Sharing and Assessment Centers (ISAC), which would monitor network activity in telecommunications, banking, and other sectors. The plan was an outgrowth of recommendations made in the October 1997 report of the President's Commission on Critical Infrastructure Protection (PCCIP) and in Presidential Decision Directive 63 (PDD 63) on Critical Infrastructure Protection issues in May 1998. Civil Rights Organizations such as Electronic Privacy Information Center (EPIC) launched a massive criticism of the plan, arguing that the authorities this way would be able to monitor all data traffic, also private e-mail, whereupon the White House stated that the plan had not yet been approved by the President and that it would be undergoing a legal review. The House committee sent the fiscal 2000 budget to the full House with language barring the Justice Department spending on FIDNET. Thus, the plan was temporarily aborted, but it will no doubt be rephrased and turn up again: This is not the first time the NSA has tried to introduce massive monitoring systems. The "Clipper Chip" was its first attempt, also under the Clinton Administration. A chip was to be installed in all telephones, modems and faxes which would make the communication content understandable to law enforcement agencies. Again, massive protests followed (sources: the civil rights organization EPIC, and the Internet journals Digi.no and ZDNet; http://www.epic.org; http://w3.digi.no; http://www.zdnet.com;http://www.wired.com

The relationship between the recent NSA initiatives and *Echelon* is unknown, but there is no doubt one.

are high: The special mobile phone which is necessary costs more than 20,000 Norwegian crowns, and you have to pay between 14 and 44 crowns per minute, depending on distance. But business can afford this when expedient, and prices will no doubt go down. In addition, the special phone can also function as a regular GSM mobile phone if a GSM net is available, and GSM prices are of course much lower. Several other similar networks will be launched shortly: Globalstar, based on 48 satellites, is planned to be launched in late 1999, and ICO, with 10 satellites (and much cheaper phones), in 2000. The satellite network Teledesic (with Microsoft's Bill Gates as one of the owners) is planned to be launched in 2003, and will be used for high velocity Internet. *The point is that Echelon's technology is apparently well suited to the interception of all of these networks.*[54]

There has been some debate and doubt as to the actual existence of Echelon (Hannemyr 1998). The reality, without the name Echelon being used, is described in great detail in several studies, such as those by Jeffrey Richelson (1995) and Laurence Lustgarten and Ian Leigh (1994). The name Echelon is used in a detailed and well documented paper as well as in a book by Nicky Hager (Hager 1996/1997, Hager 1996), who is Steve Wright's main source. The *EU-FBI telecommunications surveillance system* and the *Echelon* world wide projects may easily be partially or fully integrated: The advanced Echelon technology described above is spreading, and will soon be used within the EU-FBI efforts. The technological similarities as well as overlap and trading of personnel simply invites integration. In turn, the Quantico efforts and developments will constitute an important supportive pillar to the efforts within Schengen, with the SIS and the SIRENEs, and Europol.

Towards an Integrated System

The basic point of this paper is that there is a tendency towards convergence and integration between the various registration and surveillance systems - established or in the making - in Europe. I have given examples of such integration. Though there are obstacles and different or conflicting interests involved, the tendency has a momentum on the political as well as the policing levels.

I have also argued that the Amsterdam Treaty, which integrates Schengen into the EU structure, will give added momentum to this tendency. A Schengen formally outside the EU at least implies separate decision making bodies and structures (though, as mentioned already, the decision-making people involved are to a large extent the same, and though Schengen was originally designed as a kind of "engine" for EU in matters concerning aliens, internal order and security). A Schengen which has "disappeared" into the EU structure, will no longer have its own decision making structure, so that amalgamation with Europol, Eurodac and so on will be much closer at hand.

On the horizon we may envisage the contours of a vast, increasingly integrated multinational registration and surveillance system, with information floating more or less freely between sub-systems, at any time covering large population groups. To be sure, a full technical integration in the sense that virtually everyone in the police would have access to almost every bit of information, would easily undermine secrecy, and secrecy is a dominant police value and functional necessity. In fact, this is today considered a problem in the Schengen context by the Secret Police in several countries (for example Norway). However, as I have alluded to already, the point would be to have special branches catering to special issues, but with extensive cooperation between key people and numerous links between the various branches. Thus, the various systems which I have described could well continue to exist, and there could well be barriers between them, but the barriers would not be there for key personnel or groups of personnel, who could avail themselves of the continually expanding number of links. Judging from SIS figures today (to repeat, available sources indicate that about 700,000 persons are at present registered in the SIS), we must reckon with millions of people

[54] Well suited, but, as far as we know, not entirely without its problems. 5 August 1999 it was reported that US federal communications officials are holding up critical operating licenses for Globalstar and a handful of smaller satellite phone services while they negotiate with the FBI over wiretapping issues. The FBI and other US law enforcement agencies are worried that the new space-based phone systems, where calls may be placed from anywhere in the world, will undermine their ability to tap telephone calls. Source: Cyber Rights - http://www.cpsr.org/nii/@cpsr.org.

in a more or less integrated future system. A minority of persons will be registered because they have demonstrably committed crimes, and another minority because they are concretely suspected of crimes. A large majority will consist of people in an extremely wide circle around such persons, as well persons who in a diffuse sense are viewed as threats to public order and state security and unwanted aliens. The system will be future oriented, geared towards presumed or possible future acts.

Within the concrete context of a comparison between the Draft Convention on Mutual Assistance in Criminal Matters and the so-called "Naples II" Convention on Mutual Assistance and Cooperation between Customs Administrations, the journal *Fortress Europe?* (May 1998) arrives at the same general conclusion, and formulates it in the following telling words (pp. 6-7):

> *The complexity of this constantly developing legal labyrinth threatens to blind us to the fact that, despite their patchwork character, all of the legal and technical instruments set up in recent years in the domain of Justice and Home Affairs cooperation have one characteristic in common: each of them is in itself a paving stone on the one-way road towards the creation of a powerful common European public order and security apparatus, where the traditional border-lines between judiciary, police, customs, intelligence and military will disappear, where executive organs will play a leading role, and where national systems of checks and balances will no longer apply in a 'common area of freedom, security and justice'.*

The "common area of freedom, security and justice" referred to by *Fortress Europe?* is the title of an action plan presently under discussion in EU bodies. The JHA Council held a so-called open debate (meaning that speeches are well prepared for public consumption in advance) on the action plan at its meeting 3-4 December 1998. The action plan is geared inter alia towards implementing the changes in the areas of police cooperation and migration policies which will follow from the Amsterdam treaty. As priorities the plan for example sets out (under judicial cooperation in criminal matters) a study of "the feasibility of a European criminal record" and (under the approximation of rules on criminal matters) ensuring, within five years, that "common procedural standards should be sought that will improve mutual assistance in criminal matters. ...Consideration should be begun in the field of telecommunications interception, searches, seizures ..."[55]

As suggested in the early part of this paper, a vast, amalgamated police-based data system of the kind envisaged above may function both on the individual and the aggregate level: Individuals may be subjected to registration and surveillance, while whole population groups may quickly be sorted out for "special treatment". The system may be used for political purposes by police forces as well as through political institutions.

I have suggested that at present, Schengen is a centre of gravity among the plethora of other systems. Schengen is already on wheels. But this may change as the systems proceed towards integration: Now that Europol is operational, and when The Europol Computer Systems really get started (probably toward the end of 2001), those systems may well take the lead and become the central locus of the integrated system. The enormous potential of The Europol Computer Systems, with the various work files in addition to the central information system, as well as the development of operative functions as well as immunities and privileges on the part of Europol's personnel, suggest that Europol in the (near?) future will become a centre of power, with communication channels and power lines to the other systems.

The information stored will be so extensive that the various police and other institutions involved may experience a confusing "information overload" which they may find difficult to master. The Schengen Information System seems to have experienced this kind of difficulty. In the light of the tremendous technical possibilities, I believe, however, that this will be a beginner's problem.

[55] Sources of quotes: *Statewatch* November-December 1998, p. 2.

The Panoptical Machine - and Synopticism

In short, Michel Foucault's description of modern society as a "panoptical machine" (Foucault, Eng. ed. 1979, p. 217; original French ed. 1975) was even more apt than he thought back in 1975, when he wrote his famous book on surveillance and punishment.

The concept of "panopticism", which Foucault borrowed from Jeremy Bentham, derives from the Greek word *pan*, meaning "all", and *opticon*, which represents the visual. In a panoptical situation, a small group of observers - in principle one observer - is able to watch a whole multitude of people, and, in a panoptical society, a large segment or the whole population is similarly watched. Foucault, like Bentham before him, described the development of the modern prison as a development towards panopticism. But Foucault goes further. "In appearance", Foucault says, panopticism "is merely the solution of a technical problem, but, through it, a whole new type of society emerges" (p. 216), transported "from the penal institution to the entire social body" (p. 298). Though he did not discuss modern computerised registration and surveillance systems, his analysis may well be utilised as a theoretical framework for an understanding of the development of such systems: The likely development towards a more or less integrated, totalised registration and surveillance system in Europe implies a development towards a vast "panoptical machine" which may be used for registration and surveillance of individuals as well as whole categories of people, and which may well become one of the most repressive political instruments of modernity.

To be sure, panoptical registration and surveillance systems have existed before in history. The Church had them, the Inquisition had them, the Military had them; in a sense, they are archaic (see Mathiesen 1997 b). But never before in history have they been so inclusive, and so technically advanced and innovative, and never before in history have they developed so suddenly and rapidly: Within the span of thirty some years, the computerisation of registration and surveillance has suddenly become a reality and developed by leaps and bounds, thus reaching a new and entirely different level of sophistication, and, as I have said, a developmental tendency towards integration.

This is all the more threatening because few institutions exist which might monitor critically what is going on. The various national supervisory committees, Schengen's Joint Supervisory Authority and similar institutions, are, as we have seen, close to worthless from the point of view of control. Parliaments are not equipped with enough knowledge and insight, and not with enough power. And the mass media - the only set of institutions which in principle has significant power to monitor and even control developments - is not doing their job. In more detail:

As a parallel to the developing panopticism, there is, through the mass media, a developing *synopticism*. The concept is composed of the Greek word *syn* which stands for "together" or "at the same time", and *opticon*, which, again, has to do with the visual. Not only are we increasingly moving towards a panoptical situation where the few may see and monitor the many, we are also - especially through television - increasingly moving towards an opposite synoptical situation where many may see and monitor the few. I have outlined the details of this double development elsewhere (Mathiesen 1997 b); suffice it here to say that synopticism, where the many see the few, is also archaic: Rome's Colosseum, the emperor admired by the crowd when returning victoriously from the battle, and the Catholic priest giving his sermon from the pulpit in the cathedral are only a few of the many examples. But like the development towards panopticism, the synoptical development, through television, has accelerated tremendously in modern times. Millions, at times hundreds of millions, watch the few that television focuses on. Historically, we have seen many examples of panopticism and synopticism combined. But the historically recent acceleration of the two developmental trends shows particularly striking concurrences in time, as if they were synchronised, and striking similarities in technology as well as overlap in personnel (for details, see again Mathiesen 1997 b).

The synoptical mass media, especially television, contain great possibilities for aggressive and critical control of panoptical institutions. But the possibilities are not utilised. As the synoptical mass media developed, they became increasingly and almost unavoidably interesting as commercial targets. The commercialisation of television, and the emphasis on profit following from that, has transformed the latent possibilities of television into an enormous entertainment industry (for details, see Postman 1985) - the ancient Colosseum one thousand times enlarged. The few who are watched

by and produce messages to the many are the VIPs, the entertainers, the celebrated stars, almost a new class in the public sphere, and, on the political level, key political figures in highly staged settings. All of them become entertainers in the service of the entertainment industry, as do the participants in the many television "debates", transformed and degenerated as they are into regular talk shows. Though there are exceptions, in so-called critical journalism a president's sex life is much more important than his policies. In such a situation, the development of panopticism, though politically threatening and potentially extremely dangerous, is left almost entirely untouched. Monitoring such complex phenomena is left to the narrow journals, conferences and books, in the remote and uninfluential outskirts of public space.

At the dawn of the 21st century, this is what lies ahead in the West: A population born and raised in the age of synoptical entertainment, consequently entirely unprepared for the great potentialities of growing panoptical power.

Even more so: Reminiscent of the 1930s, extremist right wing movements are largely left unresisted and thriving by the unprepared population. Indeed, they are pushed forward by being invited to participate - and wave the flag - in the synoptical entertainment business, not because of any democratic right to participate, but because they fit excellently into the many polarised entertaining "debates" on the television stage. This is not the only reason why the right wing is on the march, but it is one of them. In the hands of an extremist right wing regime, the potentialities of panoptical power will be even greater. Watchful panoptical surveillance of and action against dissident individuals and groups, will be coupled with the political peace, quiet and absence of criticism created and maintained by the synoptical entertainment industry.

Conclusion: An Alternative Public Space?

The situation requires resistance. A full analysis of resistance strategies goes beyond the limits of this chapter (for a discussion, see Mathiesen 1982); here only this about *one* line of thinking:

The key word is, in Norwegian, "alternativ offentlighet", in German "Alternative Öffentlichkeit", in English the much more cumbersome phrase "alternative public space". The point is to contribute to the creation of an alternative public space where argumentation, well founded criticism and principled thinking represent the dominant values. I envisage the development of an alternative critical public space, whether targeted against the globalisation of surveillance or other issues, as containing three ingredients.

Firstly, liberation from what I would call the absorbent power of the mass media. I have touched on it elsewhere (Mathiesen 1996): The definition of the situation implying that one's existence is dependent on media interest, media coverage, especially television coverage. Without media coverage, with silence in the media, I presumably do not exist, my organisation does not exist, the meeting has not taken place. Relying on that definition of the situation, the actor is inescapably absorbed into the media entertainment business as the only alternative to non-existence, whereupon the content of the actor's message dwindles at the expense of his or her entertainment value. In Western society, it is probably impossible to refrain completely from media participation. At certain cross roads you are faced with a conflict: If you do not say something on television, others of the opposite opinion will fill the empty space. But it is certainly possible to be very selective, and to say "no!" to the many talk shows and entertainment-like "debates" which flood our various television channels. Most importantly, it is certainly possible not to let the definition of one's success and very existence be dependent on the media.

The second ingredient is a restoration of the self esteem and feeling of worth on the part of the grass roots movements. It is not true that the grass roots movements, emphasising network organisation and solidarity at the bottom, have died out. What has happened is that with the development of the mass media with television as their modern spearhead, these movements have lost faith in themselves. An important example from recent Norwegian history of the actual vitality of grass roots movements: In 1993, thousands of ordinary Norwegians participated in a widespread movement to give refugees from Kosovo-Albania long-term refuge in Norwegian churches throughout the country. The movement ended in a partial victory, in that all of the cases concerning

Kosovo-Albanian refugees were reviewed again by the Ministry of Justice. The example suggests that grass roots solidarity even with "distant" groups like refugees did not die out with the Vietnam war.

The third ingredient is a restoration of the feeling of responsibility on the part of intellectuals. I am thinking of a broad range of artists, writers, scientists - and certainly social scientists. That responsibility should partly be directed towards a refusal to become a part of the mass media show business. Partly it should be directed towards re-vitalisation of artistic work, writing and research taking the interests of common people as point of departure. This point is not new, but goes, of course, many decades back in Western intellectual history. The area is full of conflicts and problems, but they are not unsolvable.

In the area of penal policy, we have tried to do some if this in Norway, in the organisation KROM, The Norwegian Association for Penal Reform. KROM is a strange hybrid of an organisation, with intellectuals and many prisoners, with a common cause. By organising large conferences on penal policy every year (to create a tradition, organising them in the same place, in a mountain resort outside Oslo), with wide participation from the whole range of professions and agencies relevant to penal policy as well as many prisoners, and also by organising regular seminars and other activities, we try to create *a network of opinion and information* crossing the formal and informal borders between segments of the relevant administrative and political systems. The point is precisely that of trying to create an alternative public space where argumentation, well founded criticism and principled thinking are dominant values, a public space which in the end may at least to some extent compete with the superficial public space of the mass media.

The same may be done in the area of surveillance. Again, the public sphere of television and other mass media is not the only public sphere. The point would be for criminologists, sociologists of law and other social scientists, but also for a wide cross section of professions such as teachers, authors, songwriters, actors, musicians and so on, to develop jointly a public space of critique and discussion of the deeply disturbing issues involved. This would necessarily imply some limited participation in the public sphere of television, but mostly it would imply independent public work and publicity through the various channels of communication and networks in which such a broad spectre of professionals is involved. The *joint* character of the effort would probably come gradually, as the movement developed. The excellent journals *Fortress Europe?* and *Statewatch* constitute important beginnings, both continuously giving the precise details and in depth analyses of what is going on. In the case of *Statewatch*, activities also include use of the Internet, publication of inexpensive, informative pamphlets and so on. The expression "pamphletering" could be coined to denote a method of reaching new audiences.[56] Others would have to follow up, in and across their respective networks. Plays and novels would have to be written. A modern version of *1984* is in order. Through the development of such an alternative public space of discussion and critique of the surveillant state, warnings and information could reach sizeable segments of the population. When people are informed beyond the intricate technicalities which are so difficult to comprehend, and get a gut feeling of what is going on, they become worried and engaged. Also, considerable pressure could be brought to bear on the political system. Concern about environment and pollution – an equally technical area - developed in this way: from almost nothing to a broad and powerful movement. Why not global surveillance? The mass media, including television, might even to some extent follow suit, cynically geared as they are towards "where the action is". They did so in the area of environment and pollution. But because of its basic role in the entertainment industry, television is a distrustful ally, and great care should be taken to prevent the surveillant state from becoming an entertainment object where entertainment is figure rather than ground, to use a phrase from gestalt psychology. Entertainment may be a method to further information and engagement (remember Dario Fo), but when entertainment in itself becomes the goal, there is danger ahead. Again, the issue of environment and pollution has unfortunately in part become such an goal for television. The Norwegian soap opera "Off-shore", which pictures life and sex on an oil rig, is an example. We should learn from the errors of the past.

We should also note that an alternative public space of the kind I am suggesting has one important advantage over against television as well as other mass media: It would be based on the

[56] I owe this point to Tony Bunyan.

actual and organised relationships between people. The public space of the mass media, especially television, is in that sense weak: It is a public space which is unorganised, segmented, splintered into millions of unconnected individuals - this is its truly mass character - and equally segmented into thousands of individual media stars on the media sky. This is the Achilles' heel of the public space of the media, where an alternative public space would have an upper hand. A model - probably unattainable in practice but at least challenging as an ideal - would be the political and critical kind of *bourgeois public space* which developed in the "salons" and coffee houses of France and England through the 1700s. This was a public space which finally competed successfully with - and neutralised - the once so splendid public space of the Court and the old regime, thus preparing the grounds for the great French revolution of 1789 (Habermas 1962).

To repeat, this is one line of thinking. There are obviously others. None of the roads are broad and easy to walk. Let me conclude by saying that the expanding surveillant state, threatening the democratic fabric of our society as we know it, represents a permanent challenge to those of us concerned, politically and/or scientifically, with the sociology of social control in the widest sense of the word.

Literature[57]

Activity Report March 1995-March 1997 of the Schengen Joint Supervisory Authority.

Annual Report March 1997-March 1998 of the Activities of Schengen Joint Supervisory Authority.

Annual Report of the Central Group in Schengen (German), 26 March 1996.

Annual Report on the State of Affairs at the External Border 1 January 1996 to 31 December 1996 of the States in which the Schengen Convention has been enforced (German), published 20 March 1997.

Blume, Peter: "Schengen og personaldatabeskyttelsen" (Schengen and the Data Protection). *Social Kritik* No. 22/23 1992, pp. 64-71.

Bruggeman, W.: "Data Protection Issues in Interinstitutional Information Exchange: The Case of Criminal and Administrative Intelligence". Paper delivered at *the Sixth Schengen Colloquium: Schengen's Final Days?*, European Institute of Public Administration, Maastricht 1998.

Bunyan, Tony: *The Europol Convention*. A Statewatch publication 1995.

Campbell, Duncan: "ENFOPOL Plans Provoke Strong Opposition". *Telepolis* 31 December 1998 (http://www.de/deutsch/special/enfo/6329/.html).

Council of Europe Convention on Data Protection, 1981.

Draft Convention of the European Information System, EIS, 10 November 1993/1 December 1995.

Draft Convention on Mutual Legal Assistance in Criminal Matters, 1997.

Draft Rules of Procedure of Joint Supervisory Body of Europol, 13 October 1997.

Draft Schengen Manual on Police Cooperation in Maintaining Public Order and Security, prepared by the Schengen Working Group I on Police and Security, 11. June 1997.

Draft Convention on Eurodac, 17 April 1996 (Danish); third revision 24 November 1997.

Eskeland, Ståle: *Grunnloven og Schengensamarbeidet* (The Constitution and Schengen). Oslo: Gyldendal Publishers 1997.

EU Directive on Data Protection, 95/46EF.

Fortress Europe? A series of issues.

Foucault, Michel: *Discipline and Punish. The Birth of The Prison.* Eng. ed. New York: Vintage 1979.

Frankfurter Rundschau, 25 October 1997.

[57] The titles of reports in non-English languages are translated into English by the author. The original language is indicated in parenthesis. In addition to the literature referred to in this list, a number of documents are referred to in the text.

Frigaard, Iver: "Police Cooperation: Current Problems and Suggestions for Solutions in Interstate Co-operation in Europe". Paper delivered at *the Fourth Schengen Colloquium: Schengen and the Third Pillar of Maastricht*, European Institute of Public Administration, Maastricht 1996.
Habermas, Jürgen: *Strukturwandel der Öffentlichkeit. Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft.* Neuwied: Luchterhand 1962.
Hannemyr, Gisle: "Fantastiske fortellinger om teknologi" (Fantastic Tales about Technology). *Aftenposten* 18 March 1998.
Hager, Nicky: *Secret Power. New Zealand's Role in the International Spy Network.* Nelson, New Zealand: Craig Potton Publishing 1996.
Hager, Nicky: "Exposing the Global Surveillance System". *Covert Action Quarterly*, No. 59, Winter 1996-97.
Information (Danish daily), 3 December 1997.
Information News Letter: Information for People Working in the Ministry of the Interior, No. 1 Sept. 1997 (German).
van der Klaauw, Johannes: "The Dublin Convention: A Difficult Start". Paper delivered at *the Sixth Schengen Colloquium: Schengen's Final Days?*, European Institute of Public Administration, Maastricht 1998.
Letter from the German Ministry of the Interior to the Bundestag 1 October 1997 (German).
Lustgarten, Laurence and Ian Leigh:*I n From the Cold. National Security and Parliamentary Democracy.* Oxford: Clarendon Press 1994.
Mathiesen, Thomas: *Makt og motmakt* (Power and Counter-Power). Oslo: Pax Publishers 1992. Also available in German: *Macht und Gegenmacht, Überlegungen zu wirkungsvollem Widerstand.* München: AG Spak Publikationen 1986.
Mathiesen, Thomas: "Driving Forces Behind Prison Growth: The Mass Media". *Nordisk Tidsskrift for Kriminalvidenskab* Vol. 83 No. 2 1996, pp. 133-143.
Mathiesen, *Thomas: Schengen: Politisamarbeid, overvåking og rettssikkerhet i Europa* (Schengen: Police cooperation, surveillance and legal protection in Europe). Oslo: Spartacus Publishers 1997 a.
Mathiesen, Thomas: "The Viewer Society: Michel Foucault's 'Panopticon' Revisited". *Theoretical Criminology*, Vol. 1 No. 2, 1997 b, pp. 215-234.
Medosch, Armin: "The European Secret Service Union". *Telepolis* 30. november 1998 (http://www.de/deutsch/special/enfo/6329/.html).
Nikolopoulos, George: "Security Arrangements at the External Borders of Schengen: A View from Greece". Paper delivered at *the Sixth Schengen Colloquium: Schengen's Final Days?*, European Institute of Public Administration, Maastricht 1998.
Postman, Neil: *Amusing Ourselves to Death.* New York: Viking Press 1985.
Press Release on the Meeting of the Joint Supervisory Committee in Schengen, 12 December 1997.
Press Release on the Meeting of the Schengen Executive Committee, 15 December 1997.
Report from the German Ministry of the Interior about the Schengen Cooperation in 1996, delivered to the Federal States 5/6 June 1997 (German).
Report from the German Ministry of the Interior, fall 1995 (German).
Report on Telephone Control and Modern Telecommunications Systems (The Aukrust Report), 1996 (Norwegian).
Report to Parliament from the Commission appointed by Parliament to investigate allegations of illegal surveillance of Norwegian citizens (the Lund Report) Oslo, 28 March 1996 (Norwegian).
Richelson, Jeffry T.: *The U.S. Intelligence Commmunity.* Boulder: Westview Press 3. ed. 1995.
SIRENE manual (Danish), March 1994.
Statewatch. A series of issues.
Statewatch European Monitor. Vol 1, No 1 1998 and Vol 1, No 2 1999.
Sørbye, Espen: "Jødeforfølgelsene under den annen verdenskrig: Et mørkt kapittel i statistikkens historie?" (The Persecution of Jews during World War II: A Dark Chapter in the History of Statistics?). *Samfunnsspeilet* Vol. 12, No. 4 1988, pp. 2-17.
The Schengen Information System and it Implementation in Belgium, December 1994.
Tromp, Ruud: "The Inner Workings of SIRENE". Paper delivered at *the Sixth Schengen Colloquium: Schengen's Final Days?* European Institute of Public Administration, Maastricht 1998.

de Zwaan, Jaap: "Schengen and Its Incorporation into the new Treaty: The Negotiating Process". Paper delivered at *the Sixth Schengen Colloquium: Schengen's Final Days?*, European Institute of Public Administration, Maastricht 1998.

Webber, Frances: "Crimes of Arrival: Immigrants and Asylum-Seekers in the new Europe". Paper at *the 23rd Conference of the European Group for the Study of Deviance and Social Control*, Crossmaglen, Northern Ireland 1-4 September 1995. Published by Statewatch.

Work Programme of the Austrian chairmanship in Schengen (German), fall 1997.

Wright, Steve: *An Appraisal of Technologies of Political Control. Final Report.* European Parliament, Scientific and Technological Options Assessment, January 1998; revised report, September 1998.

Price £6.00 **ISBN 1 874481 17 2**