Preface

The Norwegian Parliamentary Intelligence Oversight Committee (the EOS Committee) is required to submit an annual report about its activities to the Norwegian Parliament (the Storting). This abbreviated annual report for 2011 presents some of the main items in the more extensive report. You can find the complete version of the annual report on the Committee's website at www.eos-utvalget.no.

Chapter I describes the Committee's mandate and composition. Chapter II provides an overview of the Committee's activities in 2011, including inspections, consideration of cases the Committee has raised on its own initiative, complaint cases and some important meetings, conferences and study visits in Norway and abroad. The Committee has submitted two special reports to the Storting. These special reports are briefly described in Chapter III. In Chapter IV, the Committee sums up some of the experience gained after 15 years of parliamentary oversight of the intelligence, surveillance and security services. Chapters IV to VIII contain information about inspections carried out by the Committee and cases involving matters of principle that the Committee has raised with the services.

In addition to ordinary inspection work, the reporting year was dominated by the work on the investigation into the methods used by what was then called the Norwegian Police Surveillance Service (POT) in the Treholt case and the Committee's first project-based investigation. This has somewhat limited the Committee's capacity to consider other cases on its own initiative. The Committee has also made efforts to increase its understanding of the services' technical information collection activities.

The services have generally demonstrated a good understanding of the Committee's oversight. Experience shows that oversight of the intelligence, surveillance and security services helps to safeguard individuals' due process protection and to create confidence that the services operate within their statutory framework.

Content

1. The Committee's mandate and composition

1.1 The Committee's mandate

The EOS Committee is tasked with continuously overseeing intelligence, surveillance, and security service (EOS service) carried out by, under the control of or on behalf of public authorities. The EOS Committee's mandate is set out in the Act relating to the Oversight of Intelligence, Surveillance and Security Services and in the Directive relating to Oversight of the Intelligence, Surveillance and Security Services. The Act and Directive were most recently amended in June 2009. The Act relating to Protective Security Services, the Act relating to the Norwegian Intelligence Service and the Instructions for Defence Security Service all refer to the Act relating to the Oversight of Intelligence, Surveillance and Security Services and state that the services are subject to oversight by the EOS Committee.

The Committee's primary function is to oversee that the EOS services do not subject individuals to unjust treatment. The Committee shall ensure that the services act within the framework of the law, directives, and non-statutory law. The oversight is primarily carried out by means of inspections of the services' archives, computer systems and installations. Subsequent oversight is practised in relation to individual cases and operations. However, the Committee has full right of inspection and shall be kept continually informed about ongoing cases. The Committee's oversight shall cause as little inconvenience as possible to the services' day-to-day activities. Particular account must be taken of the protection of sources and information received from cooperating foreign services.

The Committee shall investigate all complaints from individuals and organisations. Any complaint or enquiry that claims that someone has been unjustly treated by the services shall be investigated in the service or services that the complaint concerns.

1.2 Composition of the Committee

The EOS Committee has seven members, including the chair and deputy chair. Members are normally elected for a term of five years, but can be re-elected. The members are elected by the Storting on the recommendation of the Storting's

Presidium, but the Committee works independently of the Storting on the basis of its mandate. Members of the Storting cannot be members of the Committee. The Storting has emphasised diversity in the composition of the Committee, in terms of political background as well as experience from other areas of society. The committee members, secretariat employees and persons engaged to assist the Committee are all required to have top level security clearance.

Until 30 June 2011, the Committee was chaired by Helga Hernes, former state secretary at the Ministry of Foreign Affairs and ambassador to Vienna and Bern. Eldbjørg Løwer, former government minister and deputy head of the Norwegian Liberal Party, took over as chair on 1 July 2011. The deputy chair is Svein Grønnern, Secretary General of SOS Children's Villages Norway and former Secretary General of the Norwegian Conservative Party. The other committee members in 2011 were Trygve Harvold, former Managing Director of the Norwegian Legal Database Foundation, Lovdata; Gunhild Øyangen, former Member of the Storting and government minister for the Norwegian Labour Party; Knut Hanselmann (until 30 November 2011), former mayor of Askøy municipality and Member of the Storting for the Progress Party; Theo Koritzinsky, former Member of the Storting and head of the Socialist Left Party; Wenche Elizabeth Arntzen, District Court Judge in Oslo District Court and former advocate; and Hans Johan Røsjorde (from 1 December 2011), former County Governor of Oslo and Akershus and Member of the Storting for the Progress Party.

2. Overview of the Committee's activities in 2011

2.1 Inspections

Pursuant to Section 11 subsection 2 of the Directive relating to Oversight of the Intelligence, Surveillance and Security Services, inspection activities shall, as a minimum, comprise bi-annual inspections of the Intelligence Service headquarters, quarterly inspections of the National Security Authority, six inspections per year of the Headquarters of the Police Security Service (PST) and three inspections per year of the Defence Security Agency. Annual inspections shall also be carried out of PST

entities in at least four police districts, at least two intelligence service entities and/or intelligence/security service functions in military staffs and units and at least two security clearance authorities outside the National Security Authority.

On this basis, the Committee has carried out 26 inspections of the services, including 17 at the central level. The following nine external and local entities were inspected in 2011: PST Asker and Bærum, PST Sør-Trøndelag, PST Nordmøre and Romsdal, PST Øst-Finnmark, personnel security services at the County Governor's Office for Oslo and Akershus, personnel security services in the Ministry of Foreign Affairs, the Norwegian Armed Forces' station in Kirkenes (FSTK), the Norwegian Armed Forces' station in Fauske (FSTF) and the department for the protection of critical information infrastructure (BKI). The Committee's technical expert has participated in eight of the inspections carried out in 2011.

The services' briefings about their activities and the topics requested by the Committee are an important part of these inspections. This information provides useful insight into relevant topics, and forms the basis for specific questions and more general issues and matters of principle.

The Committee has held 23 internal working meetings during the year to prepare and follow up the inspections, and to consider complaint cases and cases that the Committee has raised on its own initiative.

2.2 Cases raised on the Committee's own initiative and complaint cases

The Committee raised 16 cases on its own initiative in 2011. The most important of these cases are mentioned below. The Committee received 29 complaints against the EOS services in 2011, which is about average for recent years. Ten of these complaints were dismissed on formal grounds, among other things because they were outside the Committee's oversight mandate or because the complaint was not sufficiently specified. However, where possible, the Committee advised the complainants in such cases about how they could pursue their case or which body they could address their complaint to.

2.3 Meetings, visits and participation in conferences

During the year, the whole Committee or some of its members have held information meetings with various public authorities and supervisory bodies in Norway and abroad. In addition, members of the Committee and the Committee Secretariat have participated in several conferences. Some of these are listed below in chronological order:

In March, representatives of the Committee Secretariat participated in a meeting for the secretariats of oversight committees for the EOS services of Sweden, the Netherlands, Belgium and Norway. In April, members of the secretariat visited the secretariat of the Swedish Commission on Security and Integrity Protection (SÄKINT) and the Swedish inspection authority for military intelligence activities (Statens inspektion för försvarsunderrättelsesverksamheten (SIUN)) in Stockholm. In May, one member of the Secretariat participated in the National Security Authority's seminar for security clearance authorities, and a member of the Committee gave a talk at the seminar about the EOS Committee's oversight of personnel security service. In May, the Committee went on a study trip to The Hague, where it met with representatives of the Dutch EOS services and the Review Committee for the Intelligence and Security Services (CTIVD). In October, three committee members participated at the 7th Conference of the Parliamentary Committees for the Oversight of Intelligence and Security Services of the European Member States, to which Norway and Switzerland were also invited. Among other things, the conference discussed different methods of informing parliament, the general public and individuals about illegal surveillance and challenges relating to the supervision of cooperation between civilian and military secret services. The conference was also informed about the web-based European Network of National Intelligence Reviewers (ENNIR). In December, some of the Committee's members met with representatives of the 22 July Commission and its secretariat, who wished to learn about the Committee's oversight of the Police Security Service and the Intelligence Service.

2.4 Special reports submitted to the Storting Surveillance of Norwegian

citizens by the Surveillance Detection Unit (SDU)

The Committee submitted a special report to the Storting on 7 February 2011 about the SDU's surveillance and registration of Norwegian citizens in Norway on behalf of the US embassy in Oslo (Document 7:1 S (2010–2011)). The report was based on an investigation conducted by the Committee on its own initiative following stories in the media about this surveillance. In accordance with the Committee's mandate, the report dealt with the Police Security Service's role in the matter. The Committee found reason to criticise the service for failing to inform the Ministry of Justice and the Committee that the service was aware of the security work at the US embassy. This criticism was supported unanimously by the Storting's Standing Committee on Scrutiny and Constitutional Affairs, and by the Storting in its session of 12 April 2011.

The Committee's investigation into the methods used by the Norwegian Police Surveillance Service (POT) in the Treholt case

The Committee submitted a special report to the Storting on 14 June 2011 about its investigation into media stories about the use of unlawful methods in the Treholt case (Document 7:2 S (2010–2011)). The investigation took place on the Committee's own initiative and had the following mandate:

'The Committee shall investigate whether the Norwegian Police Surveillance Service (POT), or another intelligence, surveillance or security service, used illegal methods in the Treholt case. If this is the case, the Committee shall endeavour in particular to clarify the extent to which such methods were used, the question of legal authority, who knew about the methods used and who authorised them.'

During its investigation, the Committee reviewed the archives of the Headquarters of the Norwegian Police Security Service (PST), the material from the criminal case against Treholt and the Storting's archive from the Lund Commission. The Committee conducted interrogations of POT employees who were involved in the Treholt case. The Committee also interviewed some former and current representatives of superior authorities, including the prosecuting authority and the Ministry of Justice. The Committee engaged the services of a police expert and a legal expert in connection with its investigation. Other experts

were also consulted. In 2011, the Committee held four extra internal meetings to consider the investigation.

The surveillance of the Treholt family's flat started towards the end of 1982, and it was partly conducted from an undercover flat in the same building. The surveillance lasted until Treholt's arrest in January 1984. The investigation showed that POT had a legal basis for the telephone surveillance. However, there was no legal basis for the audio surveillance of the kitchen, library and bedroom, the video surveillance and the seven or more searches of the flat.

Part of the Committee's investigation concerned 'who knew about the methods used and who authorised them.' The investigation showed that the Director General of Public Prosecution and the management of the Ministry of Justice were aware of the surveillance, but possibly not of the overall use of methods. It was nonetheless established that the Ministry of Justice allocated funds for POT to purchase the undercover flat, as well as for 'technical equipment' for use in the surveillance. Even if the superior authority knew about and approved the methods used, this would not constitute a legal basis for surveillance measures that require statutory authority, or that are expressly forbidden by law. The Committee obtained a legal opinion concerning the legal basis from Professor Erling Johannes Husabø. The Committee agreed with his conclusion that POT lacked statutory authority, including grounds of necessity, for the covert audio surveillance, some of the video surveillance and the repeated secret searches.

The Standing Committee on Scrutiny and Constitutional Affairs unanimously supported the Committee's conclusion that POT had acted unlawfully. The Storting endorsed this conclusion in its consideration of the report on 13 December 2011.

3. Fifteen years of parliamentary oversight of the secret services

The EOS Committee is a parliamentary grounded oversight body that was established by the Storting in an act of 1995. Its establishment was motivated by extensive public attention and political debate about the secret services and their operation. The debate led to the appoint-

ment of the Lund Commission and to the establishment of the EOS Committee. This marked the start of a new era in terms of the services' activities and public oversight of them.

In the following, the Committee will point to a few key developments since the EOS Committee started operating in May 1996. The developments described below have had a bearing on the EOS Committee's work, and thereby also on its framework, work methods and possibilities to exercise oversight.

3.1 Legal developments

Human rights

Human rights have been emphasised more strongly in many countries in recent decades. In Norway, for example, Article 110 c of the Norwegian Constitution was adopted in 1994. This article states that the authorities shall 'respect and ensure human rights'. In the Human Rights Act of 1999, Norway's international human rights commitments were given precedence over Norwegian legislation. Moreover, a 2009 amendment of the Act relating to the Oversight of Intelligence, Surveillance and Security Services instructed the EOS Committee to 'ensure... that the services respect human rights'. One of the grounds for this amendment was a wish to clearly show that human rights are of great importance to the Committee's area of oversight, and to send an important signal to the services and the general public.

The European Convention on Human Rights' Article 10 concerning freedom of expression and Article 11 concerning freedom of assembly and association are both important in relation to oversight. However, Article 8 concerning the right to respect for private and family life is particularly relevant. While it is true that public authorities can infringe on this right, such infringement requires legal authority and must be necessary, for example for reasons of national security. The European Court of Human Rights has stated that extensive secret infringement on the right to privacy must be based on specific, predictable and accessible legislation. In line with this, the Committee has focused on the intelligence, surveillance and security services' infringement on the right to privacy having a clear basis in statutory provisions and procedures. The oversight has shown and shows

that infringement in relation to Norwegian citizens do occur without the necessary legal authority.

The legal framework for the services

The intelligence, surveillance and security services are subject to more legal regulation today than they were 15 years ago. From an oversight perspective, this development has been both important and necessary. In this context, the Committee has noted that the services have generally become more concerned with due process protection and protection of privacy, without this appearing to have had a negative effect on their effectiveness and legitimacy. At the same time, stricter penal provisions have been introduced for breaching the law in the secret services' area of responsibility, and the Police Security Service (PST) has been given extended powers for preventive purposes: In 2005, PST was given the right to use telephone or internet surveillance if there is 'reason to investigate whether someone is preparing an act' falling within PST's area of responsibility, cf. the Police Act Section 17 d.

3.2 International developments

Threats from foreign intelligence services and violent groups in Norway continue to exist. But, compared with the situation 15 years ago, the present threat situation is more dominated by international terrorists who cooperate by means of modern communication technology. The fact that threats can also come from individuals ('solo terrorism') and non-governmental networks and organisations places greater demands on the services than before. It has therefore become more necessary for the Norwegian intelligence, surveillance and security services to cooperate with each other and with foreign services. This has also lead to an increase in the Committee's work of overseeing the exchange of information between the services and cooperating services. Important challenges in this context have included rules on national jurisdiction, lack of coordination between the regulatory frameworks for the different services and the services' assurances that secret information from other countries' secret services is not communicated to third parties (the 'third party rule').

Now that international cooperation between intelligence, surveillance and security services has increased, the Com-

mittee has seen the importance of contact between different countries' monitoring and oversight authorities. In cooperation with the Geneva Centre for the Democratic Control of Armed Forces (DCAF), the Committee organised a seminar in 2008 that addressed the challenges facing the monitoring and oversight authorities in relation to transboundary cooperation between the intelligence and security services. Several of these issues were followed up in the book International Intelligence Cooperation and Accountability, published in January 2011. At present, the Committee and DCAF are cooperating with a view to publishing a handbook in 2013 in which these topics will be discussed. In the years ahead, the Committee will strengthen its contact with foreign monitoring and oversight authorities through joint publications, study trips, seminars and conferences.

3.3 Technological developments

New communication channels have developed, and forms of communication that were previously separate can now be combined. This has to a certain extent changed the way in which the intelligence, surveillance and security services work. At the same time, restrictions have been imposed on the services' information collection activities. The Committee is tasked with overseeing that these restrictions are complied with. Technological progress has facilitated more effective oversight of the intelligence, surveillance and security services. It is challenging, however, for the Committee to continuously adapt its oversight activities to technological developments, among other things because technology develops much faster than the regulatory framework.

The amount of data obtained and communicated is far greater than before. How to handle surplus information and the deletion of irrelevant information have become important challenges. At the same time, it has become possible to store large amounts of information in small units, and in different locations simultaneously. The fact that the services' level of technical specialisation has increased is also very demanding for the Committee. Oversight must primarily be based on spot checks. Full oversight of the services' technical systems and data processing is not possible for the Committee to achieve.

In order to oversee the services' technical systems, the Commit-

tee has engaged the services of a technical expert. Since 1999, this expert has assisted the Committee in its oversight of the services' technical information collection, in particular by attending several of the Committee's internal meetings, seminars and inspections. In 2011, the Committee decided to use the technical expert more than it has done in the past, and even more assistance will probably be required in the years ahead.

3.4 Development of the Committee's oversight activities

Since it was established in 1996, the Committee has conducted nearly 400 inspections, raised around 200 cases on its own initiative and considered almost 400 complaint cases. The Committee has held just over 300 internal meetings during this period.

The Committee and the services now know more about each other's tasks and roles, and communication between the Committee and the services is much better than it was at first. This provides a good basis for the oversight activities and simplifies the Committee's access to information from the services. At the same time, there will always be a certain amount of tension between a secret service and an oversight committee. One way in which such tension manifests is that the intelligence, surveillance and security services do not always submit relevant information to the Committee. The Committee now invests considerable resources in searching for information held by the services that is of importance to the oversight activities. However, the Committee is also dependent on relevant information being submitted by the services on their own initiative.

The EOS Committee has been strengthened by the expansion of the Secretariat. From originally comprising of one legal employee and one clerk, both working part-time, in 1997, the Secretariat has now grown to comprise four legal advisers and one administrative adviser, in addition to the head of the Secretariat, who also holds a law degree. This has enabled more targeted and specific preparation of the Committee's inspections.

Project work has previously been initiated on the basis of specific findings by the Committee or matters exposed by the media, for example the 2009 investigation into the

methods used by what was then called the Norwegian Defence Security Service and the 2011 investigation into the methods used by the Norwegian Police Surveillance Service (POT) in the Treholt case. For some time now, the Committee has wanted to initiate more extensive projects of its own choice in order to address more general challenges and matters of principle. The first project in this category was initiated in 2011. It is described below.

In recent years, the Committee has raised several matters concerning greater insight into the services. They have gradually shown more willingness to release information to the public. The Committee has also become more aware of the importance of providing information about its oversight activities. It has therefore to an increasing extent issued press releases about cases it has been working on, and in 2011 it also held a press conference. The Committee has also replied to more enquiries from the media, given more lectures and in other ways endeavoured to make the tasks and role of the oversight committee better known to the press and politicians, as well as to private individuals. The Committee's unclassified annual reports and special reports to the Storting will nevertheless remain the Committee's most important form of communication.

4 The Norwegian Police Security Service (PST)

4.1 General information about oversight of the service

In 2011, the Committee conducted six inspections of the PST Headquarters (DSE). The Committee has also inspected the PST entities in Asker and Bærum, Sør-Trøndelag, Nordmøre and Romsdal, and Øst-Finnmark. The Secretariat now spends more time searching in archives and computer systems in preparation for the Committee's inspections. This has enabled more focused inspections. The Committee is currently considering several cases relating to the service's registration practice, including a project about how it relates to Section 15 of the PST Regulations concerning registration solely on the grounds of political, religious, philosophical etc. convictions.

The Committee has received 11 complaints against PST in 2011, compared with 9 complaints

in 2010. All complaints that were not dismissed on formal grounds were investigated in PST.

In the annual report for 2010, the Committee also stated that it had taken the initiative to clarify certain matters of principle relating to the Committee's right to inspect PST. The reason for this was that the service had, for a time, suspended the Committee's access to certain types of cases. The service reported back to the Committee that it would change its practice in accordance with the Committee's opinion. *The Committee is not aware of any cases being withheld by the service from the Committee's oversight in 2011.*

4.2 PST's use of covert coercive measures and other use of intrusive methods

General information about the use of coercive measures and the oversight of such use

Like the police, PST can request the courts to authorise the use of covert coercive measures in regular investigations. Examples of such coercive measures include communications control, covert audio surveillance, technological tracking and secret searches. PST also has the legal authority to request the use of covert coercive measures to avert criminal offences falling within the service's area of responsibility and, as the only police authority with this right, to prevent certain types of criminal offences. In addition, PST can use non-statutory methods that are not so intrusive that legal authority is deemed necessary.

The Committee's inspections of PST include regular checks of the use of covert coercive measures in individual cases. It is important to the Committee to check that petitions submitted to the courts by PST are in accordance with the service's overall information basis and whether the service uses the coercive measures in the manner authorised by the court. It is also checked that such measures are discontinued if the grounds for the court's permission cease to exist. The extent of PST's use of covert coercive measures is also a matter of interest to the Committee.

The inspections of PST's use of coercive measures in individual cases have not given grounds for criticism of PST. The Committee sees a trend towards increased use of coercive measures compared with previous

years. This applies to preventive cases in particular. During parts of 2011, PST used hidden surveillance methods in preventive cases to a greater extent than it has ever done since the service was given a legal basis for such use in 2005. In this context, the Committee refers to the legislators' intention that covert surveillance for preventive purposes shall be a limited supplement and a safety valve to be used only to prevent the most serious criminal offences. In one case (discussed below) in 2011, the Committee pointed out to PST that the nature of an operational measure was such that it required legal authority, and that the service should therefore not have implemented the measure.

Covert video surveillance of a basement storage room

In October 2011, it was claimed by the media that PST had carried out covert video surveillance of a basement storage room used by A, who was then under suspicion of conspiring with two other persons to commit a terrorist act. On this basis, the Committee, in a letter of November 2010 to PST, requested an account of the surveillance. Despite the fact that the service had kept the Committee continually informed about how the case was developing, the Committee had not been told about this video surveillance. In a letter of November 2010 to the Committee, PST confirmed that the basement storage room had been under such surveillance during the period from March/April until July 2010, when the three suspects were arrested. In the service's opinion, this was an 'operational measure', in that it consisted of video surveillance of an object in a private place, and not a coercive measure that required a statutory basis. The Committee, on the other hand, criticised the use of this method in its concluding letter in the case:

'In the Committee's opinion, the video surveillance of the storage room used by [A], including the registration, storage and logging of activities in the storage room, and the duration of the surveillance and its continuous nature, entailed surveillance of persons as regards [A] and possible third parties. The Committee can understand that PST had a strong need for information in the case, but, in the Committee's opinion, the method used could neither be justified by this need, nor by resource or efficiency considerations or the risk of discovery of an ongoing investigation . . . . In the Committee's opinion, there is no doubt that

the basement storage room was a private place and that the nature of the surveillance of persons was such that it required a statutory basis. The Committee is therefore of the opinion that PST should not have implemented the measure.'

As regards the failure to inform the Committee about the methods used in this case, the Committee stated the following in its concluding letter to the service:

'In the Committee's opinion, the nature of the covert video surveillance was such that the Committee should have been informed, and the service has therefore not fully described the surveillance measures used in this case. The Committee expects that, in future, PST will inform the Committee about all forms of intrusive methods used, including any that the service might describe as operational measures.'

The Committee will continue to monitor PST's use of intrusive methods closely, including coercive measures and the non-statutory use of methods.

4.3 Inspection of archives and registers

The archive and register inspections have accounted for an important proportion of the Committee's oversight activities in relation to PST in 2011 as well. It is particularly the requirements relating to quality of information, purpose, necessity and relevance that are subject to control by the Committee. It is also important to check that PST carries out individual assessments of the basis for registration, and that information in the intelligence register is deleted when the conditions for processing such information cease to exist.

During each inspection of DSE, spot checks of and searches in the intelligence register (Smart) are reviewed on the basis of the Secretariat's preparations. Section 3-7 third paragraph of the guidelines for PST's processing of information state in that 'intelligence registrations to which no new information has been added after five years shall be reviewed' and that 'the information shall be deleted if it is no longer required for the purpose'. The Committee's spot checks have identified cases in which the service has not deleted information even though it has ceased to be of relevance to PST. The Committee's inspection of PST's registrations of persons in 2011 resulted in the deletion of information about 73 persons.

In the annual reports for 2009 and 2010, the Committee described a case in which the

Committee had requested a written account from PST of the way in which the service practised the prohibition laid down in Section 15 of the PST Regulations, which reads as follows:

'Information about a person cannot be processed based solely on what is known about the person's ethnicity or national background, political, religious or philosophical conviction, trade union membership or information about health-related or sexual matters.'

In the same case, the Committee also raised several individual registrations in Smart with PST. PST chose to delete a large proportion of these registrations from the register. Based on this case, the Committee initiated a project in September 2011 to look more closely into registrations related to two selected milieus that PST is monitoring for preventive purposes. These registrations will, among other things, be assessed in relation to the prohibition laid down in Section 15 of the PST Regulations. *The project will be presented in a special report to the Storting in 2012.*

4.4 Disclosure of personal data to cooperating foreign services

PST has legal authority to disclose information about Norwegian and foreign citizens to cooperating foreign services. The Committee regularly checks that PST does not disclose personal data to foreign parties in contravention of the applicable regulatory framework or international human rights commitments. Among other things, the Committee checks which parties information is disclosed to, that the disclosure meets a specifically defined purpose and that the consequences for individuals are proportionate to the purpose of the disclosure. The Committee also considers the nature and quality of the disclosed information. As is known, one important aspect of the Committee's oversight is to check that information is not disclosed to states that fail to respect human rights. *On this point, the oversight in 2011 has not given grounds for criticising PST.*

4.5 PST's processing of applications for declassification and access

In several cases, PST has denied individuals access to *registered information about themselves*, as well as information that persons *were not registered in the service's registers 30 or more years ago.* The Committee has pointed out that even though the new Police

Register Act gives PST legal authority to reject applications for access, the Security Act's general provision concerning automatic declassification after 30 years will continue to apply. In the Committee's opinion, there are no good reasons for denying access to older information in cases where the special conditions for upholding classified status after such a period are not met.

The Committee contacted the Ministry of Justice in connection with this matter in 2009 and 2010. In February 2011, the Ministry confirmed that it will examine whether 'it can be confirmed that persons are not registered in the archives or registers of the Norwegian Police Security Service (PST) in the case of inquiries concerning a possible registration period that lies far back in time'. In January 2012, the Ministry informed the Committee that no further work has been done on this matter due to the Ministry's work situation following the terrorist attacks on 22 July 2011. *The Committee will follow up the matter in 2012.*

4.6 Complaint cases considered by the Committee

The Committee received 12 complaints against PST from private individuals in 2011, compared with nine complaints in 2010. All complaints that were not dismissed on formal grounds were investigated in PST. Six complaints are still under consideration. *None of the concluded complaint cases have given grounds for criticism.*

The Committee has long found that it can be a challenge to provide feedback to persons who believe that they have been under unlawful surveillance by PST, but who are unknown to the service. The Committee cannot provide information about whether or not the complainant is registered in the service's archives and registers, since this information is deemed to be classified information subject to a statutory duty of secrecy. However, in concluding some complaints cases in 2011, the Committee has, without disclosing classified information, pointed out to the complainants that the acts that the person in question believes he or she has been the victim of would have been illegal, and that the Committee would without doubt have reacted if it had uncovered such actions. This can hopefully make it easier for some people to be satisfied with the Committee's investigations.

4.7 The terrorist attacks on the government offices and Utøya

In the time since the terrorist attacks on 22 July 2011, the intelligence, surveillance and security services have kept the Committee continuously updated about their work on the case. The Committee has also carried out some searches in PST's registers and archives relating to the events of 22 July. Neither the briefings nor the searches have given grounds for follow-up. It is not within the Committee's mandate to evaluate the effectiveness of the preventive work of PST or other intelligence, surveillance and security services. In this connection, the Committee refers to the ongoing work of the government-appointed 22 July Commission and the Storting's 22 July Committee.

5 The National Security Authority (NSM)

5.1 General information about oversight of the service

The Committee carried out four inspections of NSM in 2011, including one of the NorCERT department. Control of the personnel security area was particularly important during the inspections of NSM. The Committee reviews negative decisions in security clearance cases and is briefed about various topics relating to the field. The Committee inspects NSM's electronic case processing tool for clearance cases and the directorate's records and archives.

NorCERT is the Norwegian Computer Emergency Response Team. The inspections of NorCERT showed that the department is aware of legal issues relating to the protection of privacy. The inspections did not give grounds for follow-up by the Committee. The Committee also inspected the personnel security departments of the office of the County Governor of Oslo and Akershus in January 2011 and of the Ministry of Foreign Affairs in March 2011. These inspections did not give grounds for follow-up either.

The Committee received four complaints relating to security clearance cases in 2011. One complaint was dismissed and two were concluded without criticism. In one case, the Committee expressed mild criticism of the security clearance authority.

NSM has pointed out to the Committee that the security situation in the public administration has deteriorated, and that there is a growing gap between threats and prevention. In NSM's opinion, the security work is complicated by the many uncoordinated cross-sector regulations. The Committee will take this into consideration in its further oversight of the civilian and military security services.

In the Committee's experience, the quality of case processing and assessments in comparable security clearance cases varies somewhat between security clearance authorities. This is unfortunate from an equal treatment perspective. These differences may be related to the fact that there are as many as 45 security clearance authorities in all. The number of cases processed by any one of these authorities in any one year can vary from none to several thousand. The expediency of having such a large number of security clearance authorities is questionable. This is an issue that concerns the Committee's emphasis on quality and equal treatment in security clearance cases.

5.2 The question of access to reports from security interviews

The regulations do not give a right of access to reports from security interviews before a security clearance decision is made. The Committee has stated that, considering the adversarial principle and illumination of the facts of the case, there should be such right of access. In 2010, the Committee therefore asked NSM to take an initiative in relation to the Ministry of Defence to consider whether it is necessary to amend the right of access rule in Section 25 a of the Security Act. NSM has acknowledged that it is important to avoid factual errors in such reports, and that such errors can be uncovered by allowing access. However, NSM also claims that access could be a security problem, since it can 'prevent the case from being adequately or truthfully elucidated'. Reference is also made to the fact that access can prevent 'a real and individual overall assessment of the individual's suitability', and that access before a decision is made could result in more resources being needed as well as in longer case processing times. Moreover, NSM points out that a change could result in the security clearance authori-

ties refusing to conduct security interviews. NSM concludes that right to access to reports from interviews before a decision is made should not be granted.

The Committee has taken note of NSM's assessment and conclusion. *However, the Committee cannot see that the arguments presented by NSM outweigh the need of individuals to see which facts were recorded following an interview in which they themselves participated.*

6 The Norwegian Defence Security Agency (FSA)

6.1 General information about oversight of the agency

The Committee conducted three inspections of the FSA in 2011. Among other things, the agency has informed the Committee about its protective security work, information security, operational matters and personnel security. The latter is a particularly important oversight area. The FSA is still Norway's largest security clearance authority by far. It processed more than 20,000 of the nearly 28,000 security clearance cases processed in 2011. During its inspections, the Committee reviews all cases in which security clearance was denied by the agency since the previous inspection and against which no complaint was made. In the course of a year, hundreds of decisions fall into this category.

In 2011, the Committee has reviewed several security clearance cases in which the FSA have sent authorisation forms to the persons in question in order to be able to obtain further information. In cases where the authorisation forms were not returned, the FSA denied security clearance with reference to the Security Act Section 21 first paragraph letter d (failure to present facts) without first conducting a security interview. The Committee has asked NSM, as the expert authority for personnel security, to consider whether this practice is in accordance with the regulatory requirement for a case-by-case assessment.

The Committee has received three individual complaints against the FSA in 2011. They were all concluded without criticism.

6.2 Wording of replies to complainants

On the basis of the Committee's investigation of

one particular complaint against the FSA, the agency was asked to state whether the fact that a person is not registered in the agency's registers is classified information. The background to this question was that the Committee wished to clarify in principle what information the Committee can provide in its replies to complainants who have complained against the FSA for alleged unlawful surveillance, but where the Committee finds no reason to criticise the agency. After having received the FSA's response, the Committee has concluded that its processing of such cases has similarities with corresponding cases relating to PST and the Intelligence Service: information about whether or not a person has been registered by the FSA's office for activity is classified information.

6.3 The FSA's processing of information about MC connections – bearing on security clearance

In April 2011, the Committee received a complaint against the FSA's case processing in relation to Armed Forces personnel with security clearance with negative effect for persons affiliated to Norwegian motorcycle milieus. The Committee found no grounds for considering the complaint, since it was not sufficiently individualised. However, on the basis of the complaint, the Committee decided to ask the FSA about the agency's case processing in security clearance cases where the person concerned is affiliated to a motorcycle milieu. The FSA replied that the agency carries out specific and case-by-case overall evaluations in all security clearance cases pursuant to the Security Act Section 21 third paragraph, including cases involving affiliation to a motorcycle group. The agency also stated the following:

'In the FSA's opinion, […] it is not sufficient grounds for a negative security clearance decision that the person in question is affiliated to a motorcycle group. There must be concrete evidence that the person's suitability for security clearance can be deemed to be affected by this affiliation. . . . This can be the case when the person in question associates with and has obligations in relation to known criminal elements in the motorcycle milieu. Moreover, a situation of conflicting loyalties could arise in relation to the interests of the Armed Forces in their processing of sensitive information and a motorcycle club with membership rules and a strictly enforced internal justice system.'

The Committee remarked to the

FSA that the statement was useful as a basis for further control of how the requirement for case-by-case assessments is practised in relation to this case category.

6.4 Cases from the FSA's office for activity

The Committee's annual report for 2010 described certain military counterintelligence operations (Mil CI) carried out by the FSA. In 2010, the Committee criticised the FSA for having carried out Mil CI operations in civilian areas through covert collection of information about civilians, and for failing to properly document its cooperation with PST. *In 2011, the Committee did not uncover any matters that warrant criticism relating to the FSA's military counterintelligence practices.*

Section 28 first paragraph letter e of the Instructions on Defence Security Services states that, on Norwegian territory in peacetime, the FSA shall coordinate the implementation of measures in *military areas* with a view to uncovering and preventing illegal intelligence activities targeting the Norwegian Armed Forces and its allies. Supplementary provisions to the Instructions, which entered into force on 15 July 2011, give PST sole responsibility for counterintelligence (CI) in Norway, but provide for the possibility of the FSA carrying out military counterintelligence operations in military areas and their immediate vicinity, and in military exercise areas. The rules require a clear definition in each case of what is deemed to constitute a military area. *In 2011, the Committee has kept up to date about the cooperation, and PST has informed the Committee that a draft cooperation agreement between PST and the FSA has been drawn up, in which the division of responsibility in this area has an important place.*

7 The Norwegian Intelligence Service (NIS)

7.1 General information about oversight of the service

The Committee conducted three inspections of NIS in 2011. In addition, inspections were carried out of the service's technical information collection activities at the Norwegian Armed Forces' stations in Kirkenes (FSTK) and in Fauske (FSTF). During its inspections, the Committee focuses in particular on compliance with the prohibition against collecting information about Norwegian citizens on Norwegian soil.

The Committee has also inspected the service's newly established CNO section (Computer Network Operations). The CNO section was formerly part of the Norwegian Armed Forces Information Infrastructure Agency (INI), but it has been organised under NIS since 1 January 2011. Section 6.5 of Proposition No 48 to the Storting (2007-2008) describes the CNO section's operational capability as an '[a]bility to safeguard own military information systems and exploit the opponent's systems'. Section 6.9.4 of the same document states the following is about the CNO section: 'The section helps to build the expertise and capacity required to protect the service's own information structure, and it has a certain capability to influence an opponent's information systems.' The Committee's mandate is limited to oversight of intelligence, surveillance and security functions, and it follow from the above definitions that any capabilities NIS might have in this area may fall outside the Committee's area of oversight.

The Committee routinely checks that NIS's information exchange with cooperating foreign services take place in accordance with laws and regulations and established practices. The control is described in more detail below. The Committee has received one complaint against NIS in 2011, as in 2010. *The complaint case was concluded without criticism.*

7.2 Cooperation between NIS and PST

In 2011, the Committee has kept informed about the cooperation between NIS and PST. In principle, PST's area of responsibility covers what goes on within Norway's borders, while NIS's main area of responsibility is outside the country. The services are required to cooperate in order to safeguard and protect the nation's interests. Among other things, the Committee was informed in 2011 that the services are considering whether it is necessary to revise the Collaboration Instructions of 2006, adapt further procedures for the cooperation, develop the communication system and establish a permanent liaison system.

The transfer of information between the services must take place within specified limits. The service that requests information shall ensure that the information is communicated in accordance with its statutory authority. The services may also

communicate surplus information to each other when the information is deemed to be clearly relevant to the other service. In 2011, NIS has pointed out some issues that it feels must be clarified for the future, including whether one service can obtain information in order to assist the other. In this connection, reference is made to issues relating to the limitations on PST sharing information with NIS that originate from the use of coercive measures, including the duty of secrecy rules. Such sharing of information may be necessary for NIS to be able to assist PST.

The Committee considers the issues raised to be of great importance, and it will follow them up with the services in 2012. The Committee would also like to point out the fundamental security and intelligence challenges facing PST and NIS in connection with persons who move across national borders. Section 4 of the Intelligence Service Act does not prevent NIS from carrying out surveillance or using other covert methods to obtain information about persons outside Norway. While PST needs a court ruling to use intrusive methods, the Intelligence Service Act contains few material or procedural limitations on NIS' surveillance. NIS has both a right and a duty to forward information of interest to PST to the service. This means that PST, via NIS, can gain access to methods that they would not be entitled to use in relation to persons who leave Norway – for example because the method is not permitted pursuant to the Norwegian Criminal Procedure Act, or because the court, after an overall assessment, concludes that the intrusion would be disproportionate or should be denied on other grounds. *The Committee will follow up the above-mentioned matters in 2012.*

7.3 Information exchange with cooperating foreign services

Pursuant to the Intelligence Service Act Section 3 second paragraph, NIS may establish and maintain intelligence cooperation with other countries. The Committee primarily oversees this by means of inspections of NIS's archives and communication systems. The latter is a dedicated network through which NIS receives information and shares it with its established partners in certain areas, particularly relating to international terrorism. Messages sent, received and responded to in this network can be subject to checks by the Committee.

When NIS receives enquiries from cooperating services, the service will search its own systems. If information about Norwegian citizens is retrieved during this process, it must be forwarded in anonymised form in order to prevent the identification of Norwegian citizens. The Committee also checks that personal data are only disclosed to cooperating services on the basis of specific case-by-base assessments. If NIS receives surplus information from foreign partners about cases and/or persons that fall outside of its mandate, it shall delete this information or forward it to PST.

The Committee oversees that NIS complies with the requirement laid down in the Intelligence Service Act Section 4 that the service shall not 'monitor or in any other covert manner procure information concerning Norwegian physical or legal persons'. Like PST, NIS must also continuously assess the receiving state's respect for fundamental human rights when the service exchanges personal data or other information, including when information is shared as part of Norway's participation in international operations.

In 2011, the Committee carried out searches and spot checks of messages that the service had sent to cooperating foreign services, without this giving grounds for questions in written form or criticism of the service.

7.4 The Committee's oversight of the service's technical information collection

Section 4 of the Intelligence Service Act is crucial to the Committee's oversight of the service's technical information collection. This provisions prohibits the covert procurement of information about Norwegian persons on Norwegian territory. This means that Norwegian persons must be identified as soon as their nationality has been clarified.

The legal position of Norwegian nationals who are not on Norwegian territory is not regulated by Section 4 of the Intelligence Service Act. The service is nonetheless obliged to respect the rights laid down for example in the European Convention on Human Rights Article 8 concerning the right to privacy, also outside Norway. The Committee considers it important that the service's collection of information takes place in accordance with the

objective of the Intelligence Service Act and our international commitments, and that the interests of individuals are adequately safeguarded. On this basis, it may be relevant for the Committee to consider the service's practice and its legal authority in this area in more detail.

NIS's technical information collection capabilities and methods are under continual development. Case processing and analysis tools are also continuously being updated and developed. In 2011, the Committee followed up the inspection regime that was established in 2009 whereby the Chair of the Committee has prepared all the inspections of NIS in cooperation with the Secretariat and the technical expert. During the preparatory meeting, information is provided about matters such as changes in the structure, content and functions of the technical systems, and access rights to the systems are granted in order to carry out preparatory searches and decide what is to be subjected to spot checks etc. The Committee is also presented with statistics about the information collection activities. The Committee will continue its dialogue with NIS in 2012 with a view to developing and improving the Committee's oversight in this area.

In 2011, the Committee has not found any cases of violation of the prohibition on collecting information about Norwegian citizens on Norwegian territory. Nor has it found any other matters that warrant criticism in connection with its oversight activities relating to NIS's technical information collection activities. This area will continue to be a priority in 2012.