EOS COMMITTEE

NORWEGIAN PARLIAMENTARY OVERSIGHT COMMITTEE
ON INTELLIGENCE AND SECURITY SERVICES

ANNUAL REPORT 2015

To the Storting

In accordance with Act No 7 of 3 February 1995 relating to the Oversight of Intelligence, Surveillance and Security Service (the Oversight Act) Section 8 subsection 2, the Committee hereby submits its report about its activities in 2015 to the Storting.

The annual report is unclassified, cf. the Oversight Act Section 8 subsection 2. Pursuant to the Security Act, it is up to the issuer to decide whether or not information is classified. Before the report is submitted to the Storting, the Committee sends the relevant sections of the report text to each of the respective services for them to clarify whether the report complies with this requirement. The services have also been given the opportunity to check that there are no errors or misunderstandings in the factual descriptions.

Oslo, 17 March 2016

Eldbjørg Løwer
Eldbjørg Løwer

Svein Grønnern
Svein Grønnern

Trygve Harvold
Trygve Harvold

Theo Koritzinsky
Theo Koritzinsky

Øyvind Vaksdal
Øyvind Vaksdal

Håkon Haugli
Håkon Haugli

Inger Marie Sunde
Inger Marie Sunde

Henrik Magnusson
Henrik Magnusson

The Norwegian Parliamentary Oversight Committee on Intelligence and Security Services in 2015. Left to right: Håkon Haugli, Eldbjørg Løwer (chair), Theo Koritzinsky, Svein Grønnern (deputy chair), Trygve Harvold, Inger Marie Sunde and Øyvind Vaksdal.

Contents

1. About the EOS Committee's activities in 2015 6
1.1 The Committee's remit and composition 7
1.2 Oversight activities carried out 8
1.3 External evaluation of the EOS Committee 8

2. Cases raised on the basis of attention in the public debate 9
2.1 Introduction 10
2.2 Allegations regarding fake base stations 10
2.2.1 Background 10
2.2.2 The EOS Committee's investigation into PST's use of fake base stations 10
2.2.3 PST's investigation case 10
2.3 'The mystery Mathiesen' 10

3. Developments and challenges in 2015 12

4. The Norwegian Police Security Service (PST) 14
4.1 General information about the oversight 15
4.2 Oversight of PST's processing of information in the intelligence register Smart 15
4.2.1 Brief information about the oversight 15
4.2.2 Lacking or inadequate working hypotheses 15
4.2.3 Follow-up of the basis for processing information about persons in Smart 15
4.2.4 Lacking basis for processing information about 'informants' 15
4.2.5 Change of practice for review of information about 'positive contacts' 16
4.2.6 List of email addresses in the intelligence register 16
4.3 PST's presence during the police's search of a private home 16
4.4 Old paper-based archive material found at local PST entities 17
4.5 Processing of intelligence information in the DocuLive archive system and the Smart intelligence register 17
4.6 New findings in the P area of PST's network 19
4.7 Exchange of information with national agencies 19
4.7.1 Exchange of information with the National Bureau of Crime Investigation (Kripos) – wanted alerts in the Schengen Information System (SIS) 19
4.7.2 Cooperation between PST and the customs authorities 20
4.8 Norwegian persons registered on the list compiled by the Counter Terrorism Group (CTG) 20
4.9 Notification when mobile-restricted zones are established 20
4.10 Questions about PST's processing of the Committee's complaint cases 20
4.11 Questions regarding the classification of information in cases where a complainant is aware that the PST is interested in him/her 21
4.12 Complaint cases considered by the Committee 22

5. The National Security Authority (NSM) 23
5.1 General information about the oversight 24
5.2 The Committee's work on access to Mimir 24
5.3 Case processing time for security clearance cases 24

5.4 Security interviews 24
5.5 Oversight of positive security clearance decisions in cases where the person concerned has foreign closely related persons 26
5.5.1 Introduction 26
5.5.2 Positive decisions made by NSM 26
5.5.3 Positive decisions made by the Ministry of Foreign Affairs 27
5.5.4 Conclusion 27
5.6 Complaint cases considered by the Committee 27
5.6.1 Introduction 27
5.6.2 Complaint cases 1 and 2 – long case processing time 28
5.6.3 Complaint case 3 – insufficient information about the personal history of closely related persons 28
5.6.4 Complaint case 4 – Change in disfavour of the complainant, inadequate follow-up of granted access, the requirement for grounds to be given, and long processing time 29

6. The Norwegian Defence Security Agency (FSA) 30
6.1 General information about the oversight 31
6.2 Case processing time for security clearance cases 31
6.3 Processing of personal data in the FSA's database for operational activities 31

7. The Norwegian Intelligence Service (NIS) 33
7.1 General information about the oversight 34
7.2 Special report concerning the legal basis for NIS's surveillance activities 34
7.3 The Committee's right of inspection of NIS 34
7.4 Non-conformity reports relating to NIS's technical information collection 35
7.5 NIS's procedures for deleting operational information 35

8. Oversight of other EOS services 36
8.1 General information about the oversight 37
8.2 The Committee's access to FISBasis 37

9. External relations and administrative matters 38
9.1 The Committee's external relations 39
9.2 Administrative matters 39

10. Proposals for amendments of laws and regulations 40
10.1 Deferred access 41

11. Appendices 42
Appendix 1 – Definitions 42
Appendix 2 – Meetings, visits and participation in conferences etc. 43
Appendix 3 – Act relating to Oversight of Intelligence, Surveillance and Security Service 45
Appendix 4 – Directive relating to Oversight of Intelligence, Surveillance and Security Service 46
Appendix 5 – Statement from NIS – 'the Mathiesen mystery' 49

1.
About the EOS committee's activities in 2015

1.1 The Committee's remit and composition

The EOS Committee is a permanent oversight body whose task it is to oversee all Norwegian entities that engage in intelligence, surveillance and security activities (EOS services). The Committee's remit follows from the Oversight Act and the Directive relating to Oversight of Intelligence, Surveillance and Security Service.[1] Only EOS services carried out by a public body or under the control of or on assignment for a public body, and which are relevant to issues relating to national security, are subject to oversight by the EOS Committee.[2]

Pursuant to the Oversight Act Section 2 first paragraph, the purpose of the oversight is:

1. to ascertain and prevent any exercise of injustice against any person, and to ensure that the means of intervention employed do not exceed those required under the circumstances, and that the services respect human rights,
2. to ensure that the activities do not involve undue damage to civic life,
3. to ensure that the activities are kept within the framework of statute law, administrative or military directives and non-statutory law.

The Committee shall show consideration for national security and relations with foreign powers in its oversight activities.[3] The Committee shall not seek more extensive access to classified information than warranted by its oversight purposes, and shall insofar as possible observe the concern for protection of sources and safeguarding of information received from abroad.[4] Subsequent oversight is practised in relation to individual cases and operations, and the oversight activities shall cause as little inconvenience as possible to the services' day-to-day activities.[5]

The EOS Committee has seven members. They are elected by the Storting in plenary session on the recommendation of the Storting's Presidium for terms of up to five years.[6] No deputy members are appointed. Members may be re-appointed.

The Committee is an independent body. Therefore, elected members of the Storting cannot also be members of the Committee. The Committee has a broad composition so that both different political backgrounds and experience from other areas of society are represented. The committee members and secretariat employees must have top level security clearance and authorisation, both nationally and pursuant to treaties to which Norway is a signatory.[7] This means security clearance and authorisation for TOP SECRET and COSMIC TOP SECRET, respectively. Below is a list of the committee members and their respective terms of office:

Eldbjørg Løwer, Kongsberg, chair
1 July 2011 – 30 June 2019
Svein Grønnern, Oslo, deputy chair
13 June 1996 – 30 June 2016
Trygve Harvold, Oslo
7 November 2003 – 30 June 2016
Theo Koritzinsky, Oslo
24 May 2007 – 30 June 2019
Håkon Haugli, Oslo
1 January 2014 – 30 June 2016
Øyvind Vaksdal, Karmøy
1 January 2014 – 30 June 2016
Inger Marie Sunde, Bærum
1 July 2014 – 30 June 2019

Of the seven board members, five have political backgrounds from different parties. This helps to strengthen the Committee's political legitimacy. The office of committee member is equivalent to approximately 20 per cent of a full-time position. The work as chair of the committee takes up approximately 30 per cent of a full-time position.

The Committee is supported by a secretariat, currently consisting of eleven employees. At year end 2015, the Committee Secretariat comprised the head of the secretariat, who has a law degree, six legal officers, one senior adviser in social sciences, one technological adviser and two administrative employees. The secretariat's increased capacity has not been fully utilised as intended due to long case processing time for the new staff members' security clearances and leaves of absence. The technological adviser will not start work until the

1 Act No 7 of 3 February 1995 relating to the Oversight of Intelligence, Surveillance and Security Service (the Oversight Act) and Directive No 4295 relating to Oversight of Intelligence, Surveillance and Security Service, adopted by a Storting resolution on 30 May 1995. The Act and Directive were most recently amended in July 2013.

2 References to the Oversight Act are found in Act No 10 of 20 March 1998 10 relating to Protective Security Services (the Security Act) Section 30, Act No 11 of 20 March 1998 relating to the Norwegian Intelligence Service (the Intelligence Service Act) Section 6, Instructions No 695 of 29 April 2010 for Defence Security Service Section 14, and Act No 16 of 28 May 2010 regarding Processing of Information by the Police and Prosecuting Authority (the Police Register Act).

3 Cf. the Oversight Act Section 2 second paragraph.

4 Cf. the Directive relating to Oversight of Intelligence, Surveillance and Security Service Section 5 first paragraph. It is stated in the Directive relating to Oversight of Intelligence, Surveillance and Security Service Section 6 that the Committee can make binding decisions regarding right of access and the scope and extent of oversight. Any objections shall be included in the annual report, and it will be up to the Storting to express an opinion about the dispute, after the requested access has been granted (no suspensive effect). In 1999, the Storting adopted a plenary decision for a special procedure to apply for disputes about access to Norwegian Intelligence Service documents.

5 Cf. the Directive relating to Oversight of Intelligence, Surveillance and Security Service Sections 4 and 7.

6 Cf. the Directive relating to Oversight of Intelligence, Surveillance and Security Service Section 1 first paragraph.

7 Cf. the Directive relating to Oversight of Intelligence, Surveillance and Security Service Section 1 second paragraph.

second half of 2016. The National Security Authority's long case processing time in security clearance cases concerning secretariat staff has been a problem for the Committee.

1.2 Oversight activities carried out

The Committee's oversight activities mostly take the form of announced inspections of the EOS services. The Directive relating to Oversight of Intelligence, Surveillance and Security Service requires the Committee to carry out at least 23 inspections per year.[8] In 2015, the Committee conducted 25 inspections. The Police Security Service (PST) was inspected ten times, the Norwegian Intelligence Service (NIS) five times, the National Security Authority (NSM) four times and the Norwegian Defence Security Agency (FSA) three times. The Committee also inspected the personnel security service of the Ministry of Defence and the Norwegian Communications Authority, as well as the intelligence and security functions of the Naval Special Operations Force.

The Committee's inspections consist of two parts. In one part, the committee members carry out spot checks etc. in the EOS services' computer systems, including free text searches. During the other part of the inspection, the Committee receives briefings on the services' ongoing activities and about special topics and cases that the Committee has requested information about in advance. This gives the Committee the opportunity to ask the services any questions that it finds relevant. In order to make the Committee's oversight activities more targeted, the Committee Secretariat prepares the inspections in cooperation with the services. Inspections are scheduled in meetings between the Committee Secretariat and contact persons in the services, and then confirmed in an inspection letter sent before the inspection takes place.

In 2015, the Committee has placed great emphasis on making its inspections increasingly targeted and comprehensive. No entirely unannounced inspections were carried out, but significant unannounced elements are included in many of the regular inspections. The Committee can carry out most of its oversight activities directly in the services' electronic systems. This means that the specific points that the oversight activities focus on are not known to the services before or during the inspections. The services only find out after the inspection, if the Committee writes to them. Most of the inspections carried out in 2015 gave grounds for follow-up by the Committee. The Committee raised 37 cases on its own initiative in 2015, compared with 39 cases in 2014. The cases raised by the Committee on its own initiative are mostly follow-up of findings made during its inspections.

The Committee investigates complaints from individuals and organisations. In 2015, the Committee received 23 complaints against the EOS services, compared with 26 complaints in 2014. The Committee prioritises the processing of complaints, and uses a lot of resources in this field. Some of the complaints were against more than one of the EOS services. The Committee dismissed some complaints on formal grounds, among other things because they did not fall within the Committee's oversight area. Complaints and enquiries that fall within the Committee's oversight area are investigated in the service or services that the complaint concerns. If the Committee finds grounds for doing so, it investigates complaints also in relation to other services than the one the complaint was lodged against. Generally speaking, the Committee's practice is to have a low threshold for considering complaints.

The Committee held 19 internal working meetings during 2015. At these meetings, the Committee discusses planned and completed inspections and considers complaints and cases raised on the Committee's own initiative.

The EOS services have generally demonstrated a good understanding of the Committee's oversight in 2015, as in previous years. Experience shows that the oversight helps to safeguard individuals' due process protection and to create public confidence that the services operate within their statutory framework.

1.3 External evaluation of the EOS Committee

As described in annual reports for previous years, the Committee submitted a proposal in 2013 for an external future-oriented evaluation of its activities. The basis for this proposal was that the Committee had noted a development over time in the intelligence, surveillance and security field that had consequences for the Committee's statutory oversight duties.

On 27 March 2014, the Presidium of the Storting appointed a Committee chaired by then Senior Presiding Court of Appeal Judge Bjørn Solbakken. The Evaluation Committee was tasked with evaluating the EOS Committee's activities and framework conditions. Act No 10 of 13 February 2015 relating to the committee for the evaluation of the EOS Committee released the EOS Committee from its duty of secrecy vis-a-vis the Evaluation Committee. On this basis, the EOS Committee facilitated the Evaluation Committee's work and provided requested information. The Evaluation Committee had full access to the EOS Committee's physical and electronic archives. The Evaluation Committee interviewed the committee members both individually and as a group, and also interviewed the Committee Secretariat and technical expert.

8 Cf. the Directive relating to Oversight of Intelligence, Surveillance and Security Service Section 11 subsection 2.

2.
Cases raised on the basis of attention in the public debate

2.1 Introduction

It follows from the Oversight Act Section 3 second paragraph that the Committee 'shall on its own initiative deal with all matters and factors that it finds appropriate to its purpose, and particularly matters that have been subjected to public criticism'. On this basis, the Committee has looked into some cases that have attracted attention in the public debate.

2.2 Allegations regarding fake base stations

2.2.1 Background

On 12 December 2014, the Norwegian newspaper *Aftenposten* published an article claiming that there were fake base stations for cell phones in central parts of Oslo that could be used for surveillance purposes. PST opened an investigation case on 14 December 2014. The purpose of the investigation case was to ascertain whether *Aftenposten's* material showed that unlawful intelligence activities for the benefit of a foreign state had taken place in the centre of Oslo by means of fake base stations. The Ministry of Justice and Public Security made a statement to the Storting regarding the case on 7 January 2015. PST discontinued the investigation case on 2 July 2015 with the following conclusion:

> 'The investigation activities included obtaining, reviewing and analysing *Aftenposten's* measurements and external security companies' and our own measurements from central parts of Oslo. (...) The investigation has been completed, and the conclusion is that the material obtained in connection with the investigation contains no evidence of fake base stations or IMSI catchers having been used.'

The case triggered considerable public debate, and it was questioned whether the alleged surveillance could have been carried out by or under the protection of PST. On this basis, the Committee has conducted investigations into the EOS services. Part of the purpose of the Committee's oversight is to ensure that the EOS services act within the framework of the law. It is a key oversight point for the Committee in its continuous oversight of PST to ensure that the service does not use coercive measures, including fake base stations, without court control before or after. This was also the Committee's primary function in the case in question

2.2.2 The EOS Committee's investigation into PST's use of fake base stations

The Committee carried out investigation activities in relation to PST, NIS, NSM and the Norwegian Communications Authority (Nkom). The bodies have given detailed verbal accounts, and the Committee has reviewed their systems. Separate meetings were held between PST and the Committee Secretariat and technical expert at which technical details of PST's work were reviewed.

On the Committee's request, PST has previously briefed the Committee on the service's use of IMSI catching as a method. In connection with this case, the Committee requested and received a thorough and up-to-date account of the service's use of IMSI catchers. At the same time, the Committee was given an overview of the service's use of this equipment and conducted a physical inspection of it together with the technical expert.

PST has emphasised that information received through its cooperation with the telecommunications companies was of material importance to the conclusion in the investigation case. Since this information has not been made available to the general public, the Committee has also had two meetings with the telecommunications companies. The Committee has also met with a representative of the environment that helped *Aftenposten* at the request of the person in question.

The Committee's investigation has not found that PST has used fake base stations in Oslo city centre in an unlawful manner. Nor has PST been found to accept, expressly or implicitly, the use of such methods by other parties.

The Committee will continue to monitor PST's use of IMSI catching as part of its oversight of PST's use of coercive measures.

2.2.3 PST's investigation case

In light of the public interest in the case, seen in conjunction with the Committee's purpose of ensuring that 'the activities do not involve undue damage to civic life', cf. the Oversight Act Section 2, the Committee found reason to have its technical expert review the material on which PST based its decision of 2 July 2015 not to proceed with the case. The Committee's technical expert has put a considerable amount of work into reviewing the case documents. No circumstances were identified that would give the Committee grounds for criticising PST's technical basis for the decision to discontinue the investigation.

Based on the above, the Committee concluded its consideration of the case without criticising PST.

Reference is also made to section 4.9 on notification when mobile-restricted zones are established.

2.3 'The mystery Mathiesen'

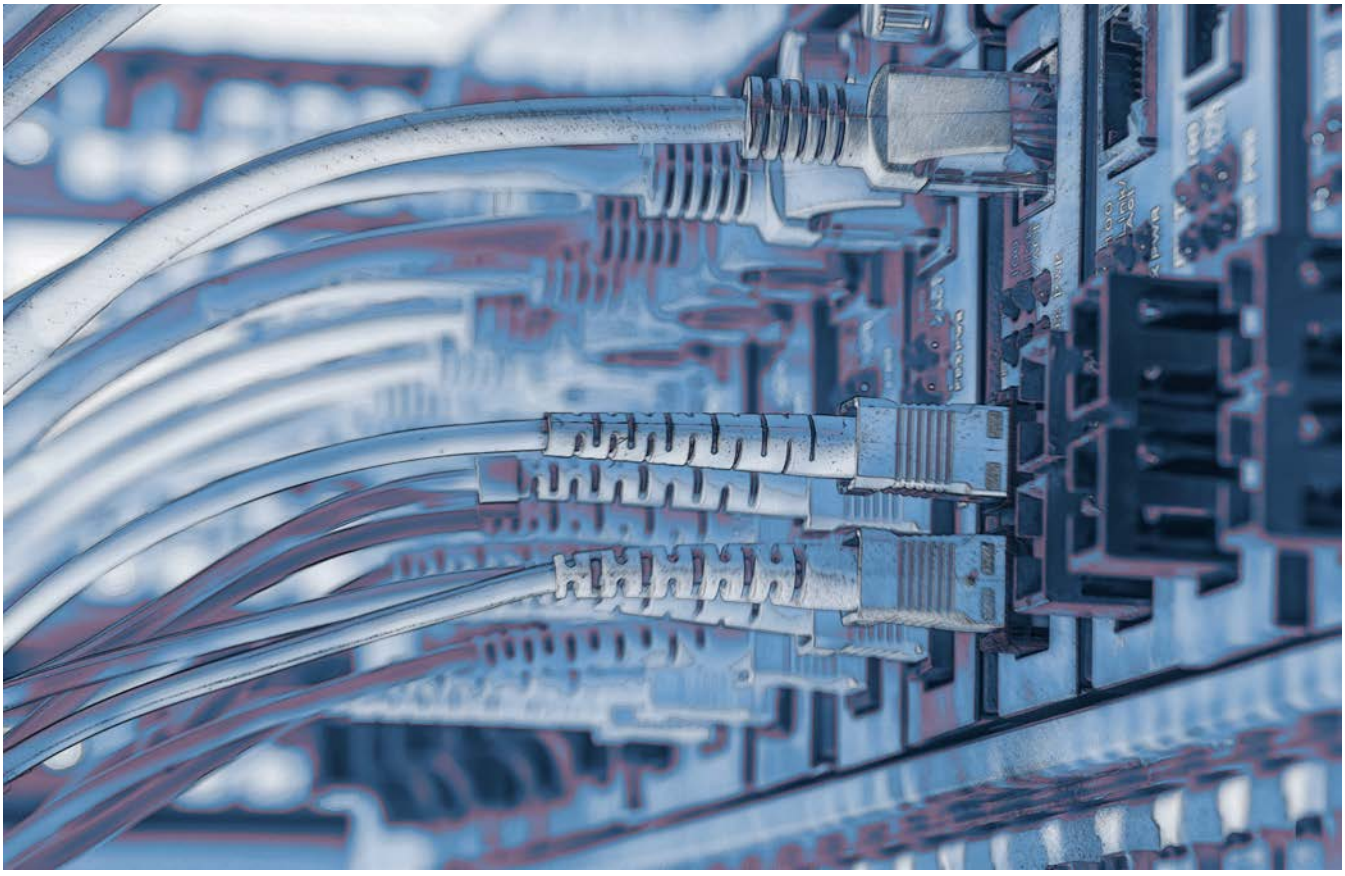
On 1 April 2015, the Norwegian financial newspaper Dagens Næringsliv (DN) published a story about 'the mystery Mathiesen'. Among other things, the article refers to the fact that in 1988, a direct telephone cable was found between the head of the intelligence service's residence and engineer Asbjørn Mathiesen's basement. The article also stated that Mathiesen had managed the intelligence service's telephone surveillance for 40 years. It was claimed that Mathiesen also

had a direct line to his basement from the Chief of Defence's home, and that he also had the possibility to listen in on the 'green network' from his own home.

The above is mentioned in sections 13.6.1, 14.2.1.4 and 14.2.1.5 of the Lund Commission's report.[9] The report describes it as giving 'cause for concern' that there was a special phone line from the head of the intelligence service's home to Mathiesen's home without the head of the intelligence service being aware of this. However, the report gives no details about why Mathiesen had this telephone surveillance opportunity and who, if anyone, knew about or initiated it. The Lund Commission's report was considered by the Storting on 16 June 1997.

In a letter dated 7 May 2015, the Committee informed the Presidium of the Storting that, following an overall assessment, it had concluded that it would not take the initiative to investigating the circumstances that DN reported in its articles. It was stated that the Committee's point of view might change should new information emerge in the case. At the same time, the Committee stated that if the Storting was to make a plenary decision ordering the Committee to investigate the matter,[10] then the Committee would of course comply with the order and request the resources necessary to carry out an investigation. The Committee has not received any feedback on the case from the Storting.

NIS later verbally informed the Committee that the service had initiated some internal investigation activities in case the Committee wanted to look into the case in more detail. It was also stated that the service believed that there might be a legitimate explanation for the cables running to Mathiesen's basement. On this basis, the NIS was asked to submit a written account. NIS's statement is enclosed in Appendix 5. The Committee has not conducted its own investigation into the Intelligence Service's statement or other aspects of the case.



9 Document No 15 (1995–1996) Rapport til Stortinget fra kommisjonen som ble nedsatt av Stortinget for å granske påstander om ulovlig overvåking av norske borgere (Lund-rapporten). ('Report to the Storting from the commission appointed by the Storting to investigate allegations of unlawful surveillance of Norwegian citizens (the Lund Report)' – in Norwegian only).

10 Cf. the Oversight Act Section 1 third paragraph.

3. Developments and challenges in 2015

In previous annual reports, the Committee has pointed to some national, international and technological developments that have a bearing on the EOS services and the Committee's oversight. Several of these developments have also been evident in 2015.

The EOS services point out in their public threat assessments that they are facing a complex and complicated threat situation. Increasingly advanced technological systems simplify information collection and analysis. This gives the services new opportunities when it comes to carrying out their tasks, but at the same time it demands a lot in terms of information processing and has a bearing on the possibilities to exercise oversight. Growing international mobility raises several issues concerning the services' persons of interest, in relation to their connection to different countries, citizenship and country of residence. While the way in which the services are organised and the division of responsibility between them assume a distinction between activities in Norway and activities abroad, the situation is more demanding in practice.

Throughout 2015, the Committee has followed the international debate about how democratic oversight of international security and intelligence work can take place. It represents a fundamental challenge that cooperation between services crosses boundaries, while oversight is limited to the national level. As a result of the Committee's interest in this issue, it has cooperated with the Geneva Centre for the Democratic Control of Armed Forces (DCAF) for a long time. In 2015 this collaboration resulted in the publication of the book *Making International Intelligence Cooperation Accountable*. The book, written by Hans Born, Ian Leigh and Aidan Wills, was partly a result of the EOS Committee's contribution, and it was launched in Oslo. The interest in transboundary cooperation in the area of oversight is slowly growing, also in the Council of Europe and in the EU. The topic has been discussed in meetings with other countries' oversight bodies, and the Committee would like to assess the possibility of coordinating an oversight investigation within the current legislative framework, i.e. of the oversight bodies of several countries investigating the same topic. Even though such an investigation would have to be coordinated at the unclassified level, it would be an opportunity to gain relevant experience of both oversight methods and what conditions must be met in order for future transboundary oversight of international security and intelligence activities to be possible.

National, international and technological developments raise many questions regarding the methods used by the EOS services. The Committee has endeavoured to continuously adapt its oversight activities to take account of these developments, but has seen that, in parallel with this, it should be evaluated whether the Committee and its oversight activities are prepared to face the challenges of the future. In the Committee's opinion, the appointment of the Evaluation Committee is crucial to ensuring the continued actual and confidence-building oversight of the EOS services. In 2015, the head of NIS pointed out that the service believes that there is a need for 'digital border control'.[11] The Committee of Digital Vulnerabilities in Society[12] proposed to prepare for public debate on the topic by producing a Norwegian Official Report (NOU).[13] If this method is established by law, the legislation must incorporate assessments of how it is to be overseen by the EOS Committee. The Committee conducts reviews of legality based on the regulatory framework in force at all times. When the EOS services are given wider powers and authorised to use extended surveillance methods, this must be followed up by a strengthening of the democratic oversight mechanisms. It is important to the Committee that the provisions authorising interventions by the services must be sufficiently clear for it to be possible to determine whether the services carry out their activities in accordance with the intentions of the legislators.

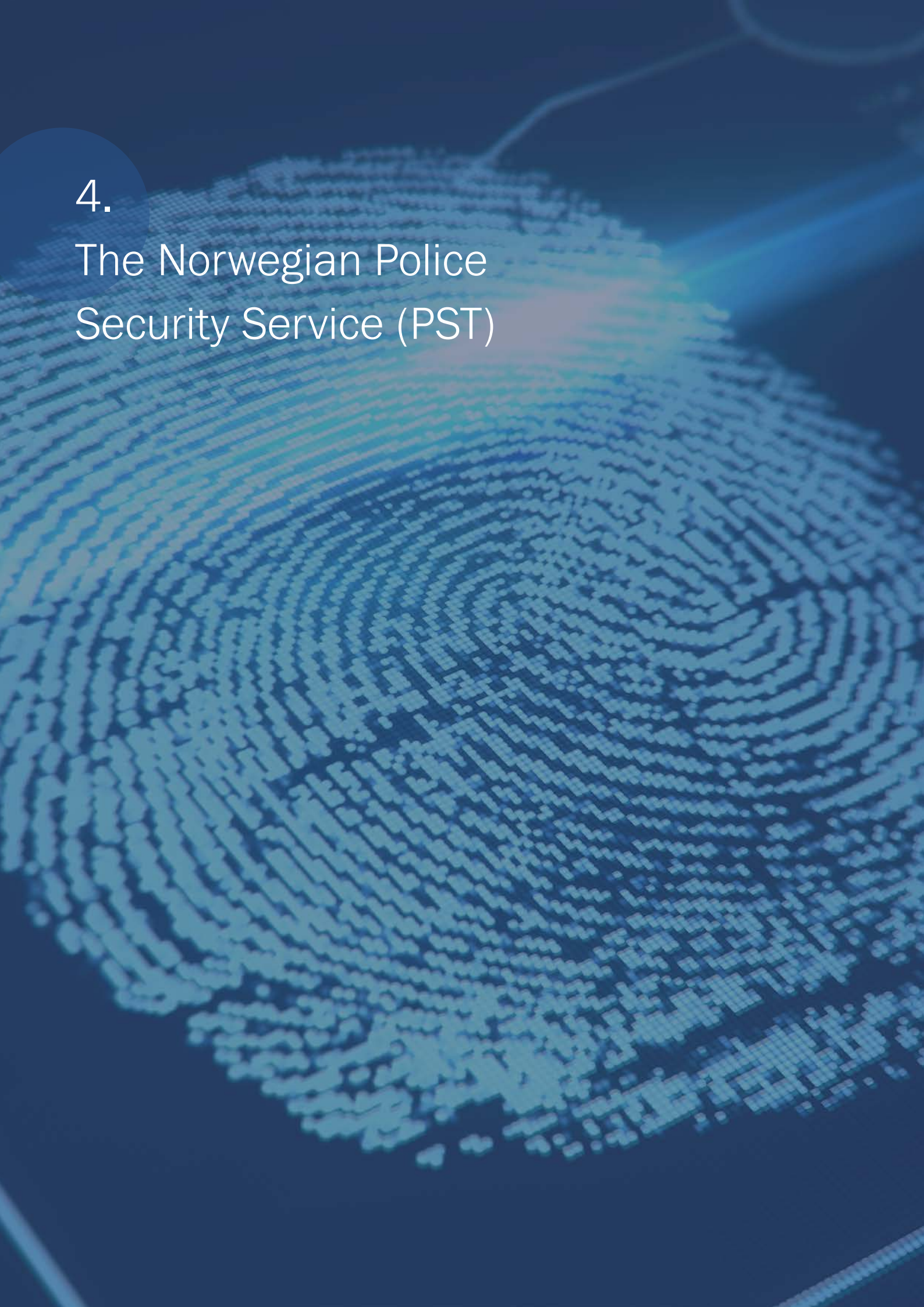
As described in section 7.4, the Intelligence Service routinely reports to the Committee on non-conformities in its technical information collection system. In 2016, the Committee will consider whether it is expedient to introduce similar procedures for other EOS services and enter into a dialogue with the services about this.

The Committee's first annual report to the Storting described it as one of its main tasks to gain the best possible insight into the activities of the EOS services. When the Committee now submits its twentieth annual report to the Storting, it can look back on significant developments, both in terms of the Committee's knowledge about the services and its possibilities of exercising oversight.

11 Norwegian Official Report NOU 2015:13 Digital sårbarhet – sikkert samfunn ('Digital vulnerability – secure society' – in Norwegian only), page 259: 'According to the Intelligence Service, it is necessary to be able to monitor relevant cable-based internet traffic in order to be able to detect, warn of and deal with foreign threats such as terrorism, espionage and cyber attacks.'

12 Norwegian Official Report NOU 2015:13 Digital sårbarhet – sikkert samfunn ('Digital vulnerability – secure society' – in Norwegian only).

13 On 24 February 2016 the Ministry of Defence appointed a committee tasked with looking into issues relating to the right to obtain information from telecommunications and data traffic into and out of Norway.



4. The Norwegian Police Security Service (PST)

4.1 General information about the oversight

In 2015, the Committee conducted six inspections of the PST Headquarters (DSE). The Committee also inspected the PST entities in Asker and Bærum, Helgeland, Hordaland and Sogn og Fjordane police districts.

In its inspections of the service, the Committee focuses on the following in particular:

- The service's computer systems
- The service's new and concluded prevention cases and investigation cases. All ongoing prevention and investigation cases are reviewed every six months.
- The service's use of covert coercive measures (for example telephone surveillance).
- The service's exchange of information with foreign and domestic partners.

During its inspections, the Committee is regularly informed about PST's ongoing activities, including the service's new prevention and investigation cases, threat assessments, and the service's cooperation with other EOS services, particularly NIS.

In 2015, as in previous years, the Committee has focused on the cooperation between PST and NIS, particularly in relation to cooperation cases and exchange of information between the services. The Committee has inspected the Joint Counter Terrorism Centre (FKTS). The Committee will continue its oversight of this collaboration in 2016, including the cooperation that takes place in FKTS.

4.2 Oversight of PST's processing of information in the intelligence register Smart

4.2.1 Brief information about the oversight

An important part of the Committee's inspections of PST is the oversight of the service's electronic systems, particularly its intelligence register Smart. The Committee regularly carries out spot checks to see whether registered information meets the requirements set out in the Police Register Act and the Police Register Regulations in terms of specification of purpose, necessity, relevance and quality. The Committee checks whether the processing information about individuals on initial registration are based on a working hypothesis, that information is not processed for longer than required for the purpose of the processing, and that information that is no longer necessary and relevant to the service's performance of its duties is deleted from the system.

Photo: Vegard Grøtt / NTB scanpix

4.2.2 Lacking or inadequate working hypotheses

The Committee has identified cases with lacking or inadequate working hypotheses. Based on this, the service prepared new working hypotheses that describe the basis on which the PST still deems it necessary and relevant to process information about the persons in question.
This is a positive development.

4.2.3 Follow-up of the basis for processing information about persons in Smart

In one case, PST registered information about a person under what is known as the four-month rule.[14] This means that it should be clarified within a four-month period whether the information was relevant and necessary to the service's performance of its duties. Nearly five years passed since the initial registration before PST followed it up. The Committee criticised PST for this.

In other cases, the Committee has seen that PST has not followed up to a sufficient extent the requirement that information shall not be processed for longer than required for the purpose of the processing. This means that the service has not been sufficiently active in its efforts to be able to assess whether it can lawfully continue to store information about a person.

4.2.4 Lacking basis for processing information about 'informants'

In the annual report for 2014,[15] the Committee stated that it had raised several cases in which PST had registered information about person classified as 'informants' without the persons themselves having been in direct contact with the service.

The Committee followed up the matter in 2015. Based on the Committee's remarks that documentation considerations

14 The Police Register Act Section 65, on time-limited exceptions from the requirements regarding specification of purpose, necessity and relevance.
15 Annual report for 2014 section 3.3.1.

alone are not a sufficient basis for processing information about an 'informant' that PST has not had direct contact with, the service reported back that it was working on ensuring documentation in other ways than by registering information about these persons in the Smart register. The Committee will keep informed about this work.

4.2.5 Change of practice for review of information about 'positive contacts'

The Committee has previously disagreed with PST's practice of excepting information about certain categories of people from evaluation under the five-year rule.[16] This has included information about PST's 'positive contacts'.

Based on the Committee's remarks, PST informed the Committee in 2015 that the service will modify its technical solutions so that these contacts are also subject to five-year evaluations. *The Committee is satisfied with this.*

PST has also informed the Committee that, based on its remarks, the service has reviewed the information about all its contacts. The review resulted in a significant reduction in the number of persons with contact status registered in Smart. *The Committee is satisfied with the review.*

4.2.6 List of email addresses in the intelligence register

The Committee has previously criticised the service for processing lists of telephone numbers with personal data about many persons in the service's systems without carrying out individual assessments before processing the information in the Smart register.

In 2015, the Committee requested that PST explain the legal basis for processing a list containing several hundred email addresses in the Smart register. Many of the email addresses could be directly linked to Norwegian individuals. Based on the service's reply, the Committee remarked that it could not see that any individual assessments had been carried out before the email information was processed. The information had thus been processed in violation of the regulations.[17] The Committee stated that it is unfortunate that PST processed email information that can be directly linked to individuals over a five-year period without the conditions for processing being met. PST deleted the list email addresses.

4.3 PST's presence during the police's search of a private home

During the review of a PST prevention case, the Committee noted that PST officers had been present during a search of a private home by the ordinary police. Photographs from this search were included in PST's preventive case against the person.

Covert searches of private homes are prohibited in cases in the preventive track. This follows from the Norwegian Constitution Section 102, cf. the Police Act Section 17d second paragraph last sentence. The Committee therefore raised with PST the matter of the service's involvement in the search and seizure carried out by the ordinary police.

PST explained that the service had had the person in question under surveillance. The ordinary police decided to arrest the person and search the person's home on the basis of a tip received from PST. The service was notified of the arrest and search of the home because the police was aware of PST's concerns regarding the person in question. According to the service, 'it was natural for PST to be present during the search (...) as an observer and in a supporting capacity'. The service also stated that it had not made any seizures during the search, but had received a copy of mirrored data from the search for independent review, as the material seized could also be of relevance to PST.

In its concluding statement to PST, the Committee remarked that the service has an independent responsibility to not request information that the service cannot lawfully obtain for itself, and that its cooperation with the police must be organised accordingly. The Committee also stated:

> 'The Committee has no information about how the search was conducted in practice or what the PST officers did there, nor about whether the ordinary police carried out the search with PST's purpose in mind as well as their own. Nonetheless, the fact remains that PST has obtained material that the service would not have had the legal authority to obtain for itself in connection with the prevention case.
>
> Although PST can receive surplus information from the ordinary police, the Committee finds that it could be problematic that PST has been present during the search in which the alleged surplus information was obtained. Since PST was present, the Committee cannot rule out the possibility that the police may have taken PST's need for information into consideration during the search and therefore secured information that PST itself does not have legal authority to obtain for preventive purposes.
>
> In the Committee's opinion, the link between the ordinary police's use of methods in the investigation case, PST's presence during the search and the subsequent transfer of information about seizures in the case from the police to PST makes the Committee's oversight of the lawfulness of PST's actions demanding.'

The Committee could not find any documentation that met the documentation requirement in relation to the requests from the ordinary police to PST for assistance in the search and review of the material seized. Nor could it find that it was shown in the police documents that the material seized had been analysed by PST and that some of it (mirror copy)

was transferred to the service as surplus information. PST acknowledged that the request for assistance received from the ordinary police should have been documented and that the service could have contributed to this. The head of PST therefore distributed an information memo to all local PST entities to ensure a better and uniform practice in future. *The Committee takes a positive view of this.*

In conclusion, the Committee made the following statement:

> 'The Committee would like to remark that it is important that cooperation with the police is organised in such a way that the PST's regulatory framework is not circumvented. If PST carries out a covert search of a private home for preventive purposes with the assistance of the ordinary police, this would be highly unfortunate on grounds of principle. This emphasises the importance of proper documentation in connection with cooperation of such a nature as in the present case.'

4.4 Old paper-based archive material found at local PST entities

During an inspection of a local PST entity in 2015, the Committee reviewed the entity's physical archive. The review showed that there was a lot of material stored in (and outside) the vault that appeared not to be of relevance to the service at present and that should have been transferred to the PST Headquarters and/or shredded. The Committee has not seen old archive material in such considerable quantities in recent years. The Committee criticised the PST entity for having inadequate procedures for the storage, transfer and shredding of old archive material. The PST Headquarters followed up the case in relation to the district in question and raised the topic with all police districts on a general basis.

Based on the Committee's findings of old archive material in recent years, the Committee requested a general account from PST of what kinds of old archive material the service believes it can store. PST gave the Committee a comprehensive and useful account of the transfer of archive material from PST to the National Archives. Among other things, the service informed the Committee that the PST Headquarters obtained archive material from local entities for the period until 31 December 1994. There should be no need for local paper archives for the period from 1 January 2010 until the present, as the case processing system has been fully electronic since 2010. The Committee took note of the account.

4.5 Processing of intelligence information in the DocuLive archive system and the Smart intelligence register

The registration of personal data and intelligence information in the archive system DocuLive raises particular issues in relation to the requirements for processing of personal data

16 Annual report for 2014 section 3.3.1.

17 Cf. Sections 13 and 14 of the PST Regulations in force at the time (now the Police Register Act Sections 64 and 6).

stipulated in the Police Register Act. The Standing Committee on Scrutiny and Constitutional Affairs' recommendation to the Committee's annual report for 2014[18] endorsed the Committee's opinion that personal data obtained by the service should be entered in the Smart register. The Standing Committee asked the Ministry of Justice and Public Security to clarify the relationship between the storage obligation set out in the Norwegian Archives Act and the Police Register Act's provisions on deletion.

PST gave the Committee a more detailed account of the relationship between the storage obligation set out in the Norwegian Archives Act and the Police Register Act's provisions on deletion. The Committee also received copies of a letter from PST to the Ministry of Justice and Public Security and a letter from PST to the National Archives about the same topic. Important clarifications will now be made, partly thanks to the Committee's interest in the matter.

PST 'understands the legal point of departure to mean that, in practice, the main rule as regards deletion pursuant to the Police Register Act will be the same for PST as for other police entities, namely that deletion takes place in the form of archive storage', regardless of where the information was initially registered, whether in DocuLive or in Smart. PST understands and accepts that personal data that must be deleted pursuant to the Police Register Act, but stored pursuant to the Archives Act, shall not be available for intelligence purposes, and stated that the service would contact the National Archives and the Ministry of Justice and Public Security to discuss possible practical solutions.

One challenge that remains is to implement a satisfactory restriction regime[19] for access to information that shall no longer be available for intelligence purposes or operational activities.[20] It remains unclear how and when restriction of access, storage and, if relevant, transfer to the National Archives are to be implemented. Other unclarified matters include procedures for different forms of deletion, and special problems relating to the processing of tips and elimination of information that is not relevant to PST's activities after four months.

The Committee made the following statement to PST:

> 'The Committee still agrees with PST that documents received and other incoming information, for example in the forms of tips, shall be stored and preserved in accordance with the archives legislation.
>
> The Committee has referred to the fact that if a tip results in a person being registered in Smart under the four-month rule, cf. the Police Register Act Section 65, cf. Section 8, and PST finds after four months that the information is not relevant and necessary to PST, the registration and all the information it includes shall be destroyed. This also applies to any documents/notes etc. that mention the person and that PST has prepared during its work to clarify whether the tip is relevant to the service (in logs, tip cases, log cases, work rooms (...) etc.).
>
> When archives legislation nevertheless requires the actual tip to be stored, the Committee is of the opinion

that it must be possible to indicate in DocuLive that the tip has been followed up by PST ('Tip followed up – not relevant to PST').'

The Committee stated that it awaits the outcome of the service's dialogue with the Ministry of Justice and Public Security and the National Archives about the above-mentioned matters. The Committee assumed that its previous remarks will be incorporated into the service's dialogue with the National Archives and the Ministry.

4.6 New findings in the P area of PST's network

In the three previous annual reports, the Committee has criticised PST for processing intelligence information and personal data outside of the established computer systems.[21] Information found in the P area[22] of PST's computer network was described in the annual report for 2014.

During one of its inspections in 2015, the Committee found that PST was still processing intelligence information and personal data in three documents in the P area of its network. The documents were forwarded to the Committee by PST together with a brief description of the findings.

In its concluding letter to PST, the Committee noted that the documents ought to have been found during the previously announced review of the P area. The service apologised and stated that the documents would now be deleted.

The Committee concluded that the P area had not been satisfactorily reviewed and cleared of intelligence information and personal data after the Committee criticised this processing in 2014. The Committee assumed that all intelligence information and personal data will be deleted from the P area.

4.7 Exchange of information with national agencies

4.7.1 Exchange of information with the National Bureau of Crime Investigation (Kripos) – wanted alerts in the Schengen Information System (SIS)

In the annual report for 2014,[23] the Committee expressed concern that all requests made by PST to Kripos in the period from 2009 to 2014 for wanted alerts in SIS had been registered without Kripos carrying out the quality control required under the Act relating to the Schengen Information System (the SIS Act). The basis for this was that PST did not want to give Kripos classified information. The Committee asked PST to consider the possibility of giving a limited number of personnel at Kripos's SIRENE bureau security clearances at the appropriate level and access to a secure information system to enable Kripos to quality assure PST's requests in future.

In the Committee's opinion, the SIS Act requires the SIRENE bureau to be given access to the underlying documentation required to check that the necessary legal authority is in place and that the conditions for registration in SIS set out in Section 8 of the Act are met. It is the Committee's opinion that if the service fails to forward the necessary underlying documentation for the wanted alert, other than a note that the conditions are deemed to be met, then the wanted alert cannot be registered. The Committee pointed out that the regulatory framework must be amended or clarified if special rules are to apply to PST's use of SIS. The Ministry of Justice and Public Security seems to express the same opinion in a letter to PST with a copy to the Committee. *The Committee has requested that the Ministry confirm its understanding of the legislation directly to the Committee.*

In the meantime, PST has been in dialogue with Kripos about a new practice for the content of SIS requests from PST to Kripos. The service will 'give somewhat more comprehensive, but still general, grounds for the request for registration', and these grounds will be unclassified. The Committee will oversee whether the content of the new grounds will enable the personnel responsible for registration to make a proper assessment of whether the conditions for registration in SIS are met.

The Committee has also expressed, in relation to both PST and the Ministry, that legal clarification is needed of the concept 'prevention' in the SIS Act in relation to the concept of 'prevention' in PST's regulatory framework. The reason for this is that the threshold level set in the SIS Act is higher than the one on which PST bases its work, which means that prevention in PST does not necessarily constitute sufficient grounds for SIS registration. *The Committee has asked the Ministry to clarify the relationship between the two concepts as they apply to PST's requests for SIS registration of people for preventive purposes.*

The Committee will revisit the matter in next year's annual report.

18 Recommendation No 289 to the Storting (2014–2015) Chapter 2 Komiteens merknader ('the Committee's comments' – in Norwegian only), page 19.

19 Restriction of access to information: Marking of stored information for the purpose of limiting future processing of the information in question, cf. the Police Register Act Section 2 subsection 10.

20 Cf. the Police Register Regulations Section 22-3.

21 See Chapter IV section 3 of the annual reports for 2012 and 2013, and section 3.4 of the annual report for 2014.

22 The P area is a network station in principle only meant to contain program files.

23 See section 3.10.2 of the annual report for 2014.

4.7.2 Cooperation between PST and the customs authorities

In the annual report for 2014,[24] the Committee commented on its investigation into the cooperation between PST and Norwegian Customs, among other things in relation to requests for customs inspections and exchange of information about individuals who cross Norway's borders, and about disclosure of information from Norwegian Custom's customs declaration system TVINN. Among other things, the Committee was of the opinion that the regulatory framework should be clearer if Norwegian Customs is to disclose information to PST in connection with cases in the preventive track.[25]

The relevant provision in the Customs Act was clarified in the Storting's bill of 29 May 2015.[26] Among other things, the amendment means that the Directorate of Customs (TD) can also disclose information to PST for use in preventive activities. It is stated in the comments to this provision that when PST requests information, TD shall assume that the conditions for disclosing confidential information are met.[27] The service will thereby gain access to necessary information without having to give detailed grounds, thus avoiding having to declassify classified information for this purpose.

It is a positive development that the legal basis for TD disclosing information to PST has now been clarified.

4.8 Norwegian persons registered on the list compiled by the Counter Terrorism Group (CTG[28])

In its annual report for 2014, the Committee stated that it had raised questions relating to the registration of Norwegian persons on a list prepared in connection with the European cooperation in the Counter Terrorism Group (CTG). PST had contributed information about dozens of people, and acknowledged in response to the Committee's questions that its follow-up of the list could have been better.

PST reviewed the list in question in 2015 and submitted the most recently updated list to the Committee. PST removed several persons who no longer met the criteria for being included on the list. The Committee has reviewed the list and found no grounds for further follow-up. The Committee has requested that the list be submitted every time PST adds or removes persons, so that the Committee can check whether the criteria for inclusion on the list are met in connection with its inspections.

4.9 Notification when mobile-restricted zones are established

The annual report for 2014 explained the provision in the Electronic Communications Act[29] Section 6-2a that requires the police, including PST, to notify the Norwegian Communications Authority (Nkom) when establishing 'mobile-restricted zones'. The Committee reported that it carries out regular oversight activities relating to the use of methods in individual cases, and that it would follow up PST's notification of Nkom.

The Committee followed up PST's notifications to Nkom in 2015, and has found no grounds for further follow-up other than the ordinary continuous oversight of the service's use of methods.

4.10 Questions about PST's processing of the Committee's complaint cases

The Committee has in 2015 raised with PST some questions about what investigative steps the service should take in connection with complaint cases considered by the Committee, and what information the Committee needs access to in order to be able to carry out its own investigation of complaint cases in a satisfactory manner.

Among other things, PST referred to the fact that the service does not routinely conduct searches in PST's system for intelligence source handling (Kildesys) when investigating the Committee's complaint cases. The service noted that the Committee was aware of this, which the Committee confirmed.

The Committee asked PST to forward all information the service possesses about a complainant when PST investigates the Committee's complaint cases. This applies regardless of which electronic or paper-based registers, archives, systems, computer areas etc. information about the complainant has been processed in, and regardless of how the service has processed the information (electronically, manually, as text, sound or visual recordings/photos etc.).

Since the Committee also conducts its own investigation of complaint cases received in relation to PST, it was requested that the Committee be given access to all electronic and paper-based registers, archives, systems, computer areas etc. that the Committee does not already have access to, including Kildesys. In this connection, reference was made to the fact that the Committee expects PST to separate the identity of sources from Kildesys so that the Committee can conduct independent searches in the system without the names of sources becoming known to it. At the same time, the Committee commented that access to these registers etc. will also be used in its other oversight activities.

Finally, the Committee took note of the fact that no written procedures exist to describe how PST should investigate complaint cases that the Committee is investigating in relation to the service. PST has stated that the service will prepare a process description for this work. The Committee expressed a positive view of this.

4.11 Questions regarding the classification of information in cases where a complainant is aware that the PST is interested in him/her

In connection with an inspection of the PST Headquarters in 2015, the Committee requested a briefing on PST's use of preventive interviews. As part of this briefing, PST was asked to explain whether it is still classified information that the service has processed information about an individual when PST officers have made themselves known by conducting a preventive interview with the person in question. The background to the Committee's interest in this matter is that it has considered complaints against PST from persons who have found out through preventive interviews etc. that PST is interested in him/her. According to the Oversight Act, the general rule is that statements to complainants shall be unclassified.[30] This means that the Committee cannot give the complainant any information about the circumstances surrounding the interview with PST, nor give any form of confirmation of PST's involvement in the interview.

PST wanted to provide written feedback on its practice. The service stated that a specific assessment of damage pursuant to the Security Act Section 11 determines whether it is classified information that PST is processing information about a person. The service also referred to the fact that, pursuant to the Police Register Act Section 66, there is no duty to provide information and the person registered has no right of access. If the Committee is to be able to confirm that a person is registered in PST's registers after a preventive interview has been carried out, that would amount to discrimination between those who contact PST directly and those who complain to the EOS Committee. PST is of the opinion that the practice of only informing the complainant about whether or not a complaint resulted in criticism must therefore be continued, also for complainants that PST has been in contact with.

In its concluding letter to PST, with a copy to the Ministry of Justice and Public Security, the Committee referred to the main rule set out in the Oversight Act that '[i]nformation concerning whether any person has been subjected

24 See section 3.10.1 of the annual report for 2014.

25 Cf. the Customs Act Section 12-1 second paragraph letter b or letter f first alternative.

26 Bill 64 (2014–2015).

27 Proposition No 52 to the Storting (Bill) (2014–2015) section 12.3 Merknader til endringer i tolloven ('Comments to amendments to the Customs Act' – in Norwegian only)

28 The Counter Terrorism Group (CTG) is a European forum for counter terrorism collaboration between the security services of the EU states, Norway and Switzerland.

29 Act No 83 of 4 July 2003 relating to Electronic Communications (The Electronic Communications Act).

30 Cf. the Oversight Act Section 8.

to surveillance activities shall be regarded as classified *unless otherwise decided*' (the Committee's emphasis). The Committee also referred to the Directive relating to Oversight of Intelligence, Surveillance and Security Service's provision that statements to complainants 'should be as complete as possible without revealing classified information'.[31] The Committee noted that the Ministry has previously expressed the opinion that, in some cases, the need to clarify to the complainant what has happened is so great that an exception must be made from the principle that no grounds shall be given for statements to complainants.[32]

If PST has conducted a preventive interview with a person and the person in question lodges a complaint with the Committee regarding the interview and/or other matters, there is an argument to be made for allowing the Committee, to a certain extent, to confirm the service's interest in the complainant and state that the Committee has considered the concrete matters that the complaint concerned. The Committee's point in relation to cases where no criticism is made is that it should at least be able to tell the complainant that the Committee has investigated the 'matters the complaint concerns' in relation to PST, alternatively combined with a statement to the effect that the Committee cannot say anything about any information PST may be processing about the person in question.

It will be particularly challenging for the Committee in such complaint cases to not even be able to confirm that a preventive interview has taken place and that the Committee has investigated information processed in that connection. In such cases, it would be natural to tell the complainant something about what has been investigated or to give more detailed grounds for the Committee's conclusion.

In its concluding letter, the Committee stated that in such cases it may be relevant to ask PST for a specific assessment of whether more detailed grounds can be given to the complainant. The service is now far more open in its approach to relevant persons than it was when the regulatory framework for the EOS Committee was created more than 20 years ago, and this should result in the Committee also being given this opportunity in certain cases, or at least in the service making a concrete assessment.

4.12 Complaint cases considered by the Committee

The Committee received 14 complaints against PST in 2015, compared with 13 complaints in 2014. One of the cases that the Committee concluded in 2015 gave grounds for criticism. The matter that was criticised has been brought to an end.

The Committee's statements to complainants shall be unclassified. Information concerning whether any person has been subjected to surveillance activities shall be regarded as classified unless otherwise decided. The Directive relating to Oversight of Intelligence, Surveillance and Security Service states that statements given in response to complaints against PST shall only state whether or not the complaint contained valid grounds for criticism.[33]

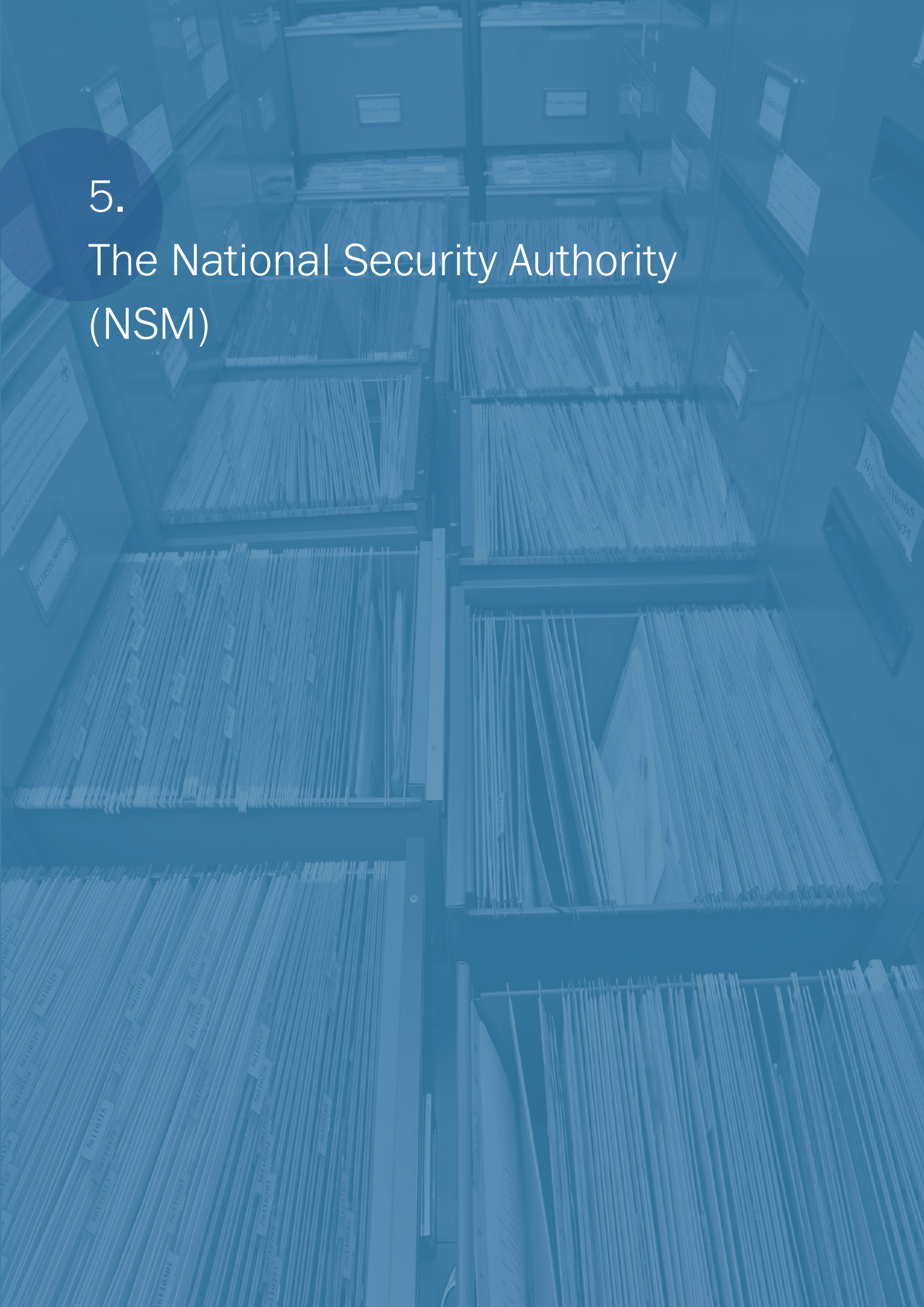
The Committee submitted a request to the Ministry of Justice and Public Security for the complainant in the case that gave rise to criticism to be given more detailed feedback, cf. the Directive relating to Oversight of Intelligence, Surveillance and Security Service Section 8 second paragraph. The Ministry concluded that it could not declassify the information about the grounds for the Committee's criticism. The Committee was thus unable to give the complainant any information other than that the complaint gave grounds for criticising PST. As a result of this, the Committee cannot provide further information to the Storting either.

The Committee's limited possibility to give complainants grounds for its criticism of PST in complaint cases represents a great challenge to the Committee. Reference is also made to section 4.11.

31 Cf. the Directive relating to Oversight of Intelligence, Surveillance and Security Service Section 8 second paragraph first sentence.

32 Report No 39 to the Storting (1992–1993) p. 43 section 8.3.1, cf. corresponding statement in Norwegian Official Report NOU 1994:4 section 7.2.4.

33 Cf. the Directive relating to Oversight of Intelligence, Surveillance and Security Service Section 8 second paragraph: 'Statements to complainants should be as complete as possible without revealing classified information. Statements in response to complaints against the Police Security Service concerning surveillance activities shall however only state whether or not the complaint contained valid grounds for criticism. If the Committee holds the view that a complainant should be given a more detailed explanation, it shall propose this to the Ministry concerned.'



5.
The National Security Authority (NSM)

5.1 General information about the oversight

In 2015, the Committee conducted four inspections of NSM. The inspections of NSM mainly focus on personnel security. The Committee's oversight activities have a particular focus on cases where security clearance has been denied, reduced or suspended by the security clearance authorities. In addition to being the security clearance authority for all CTS (Cosmic Top Secret) clearances in Norway, NSM is also the appellate body for lower security clearance levels. NSM attends to the general functions within the protective security services pursuant to the Act of 20 March 1998 relating to Protective Security Services (the Security Act). NSM's collaboration with other EOS services is also an important oversight point.

NSM is one of a total of 43 security clearance authorities in Norway. On 19 May 2015, the Ministry of Defence distributed for consultation proposed amendments to the Security Act, which included a proposal to significantly reduce the number of security clearance authorities. In the consultation memo, reference is made to differences in the number of cases considered by each body and the fact that a high number of security clearance authorities 'entails challenges as regards to the quality and efficiency of case processing'. The Ministry also expressed concern that the smaller security clearance authorities were unable to maintain the level of competence required to ensure that its case processing is of sufficiently high quality. In its consultation submission to the Ministry, the Committee stated that it supported a reduction in the number of security clearance authorities. Such a reduction can help to strengthen security clearance authorities, which could contribute to improving the due process protection of individuals as well as the general public's confidence in satisfactory case processing and equal treatment in an administrative process which is partly exempt from public access.

5.2 The Committee's work on access to Mimir

The Committee is continuously working to improve its oversight methods, including its access to the services' electronic systems. In its annual report for 2014, the Committee described its work to gain access to the fully electronic case processing tool for security clearance cases (Mimir). In the Committee's opinion, it is important that the EOS services take the Committee's oversight needs into account already when new case processing systems are being developed. The Committee needs access to security clearance cases to be able to prepare and carry out inspections, and to process complaint cases and cases raised on the Committee's own initiative. In order to ensure that the Committee is able to oversee security clearance cases during its inspections of NSM, the directorate placed a separate office with seven computers at the Committee's disposal in 2015. The Committee is satisfied with this solution.

5.3 Case processing time for security clearance cases

In its annual reports for 2011, 2012 and 2013, the Committee pointed out that the case processing time for many security clearance cases is much too long. After the situation deteriorated further in 2014, the Committee was of the opinion that the case processing time for many cases is so long that it amounts to an unreasonable encroachment on the lives of individuals by the authority. On this basis, the Committee requested in its annual report for 2014 that the Storting consider the long case processing time for security clearance cases as a separate case, cf. the Directive relating to Oversight of Intelligence, Surveillance and Security Service Section 13 subsection 3 letter g. In its recommendation to the annual report, the Standing Committee on Scrutiny and Constitutional Affairs stated that it gives cause for concern that the situation deteriorated in 2014 despite the Committee's previously expressed expectation that the situation be improved.[34] On this basis, the Committee requested that the Ministry of Defence take immediate action to remedy the situation.

In 2015, NSM informed the Committee that it had taken note of the criticism in the annual report and was working to reduce case processing time, both in security clearance cases where NSM made the initial decision and in cases it considers in its capacity as an appellate body. NSM has also informed the Committee that the case processing time remain long in 2015 because of the considerable backlog at the beginning of the year. The oldest cases have been given priority, but since they have already waited a long time to be processed, the average case processing time has gone up because it is measured by when each case is closed.

The Committee concludes that NSM has implemented measures that have reduced the backlog and expects the case processing time of more recently received cases to be shorter. The Committee notes that security clearance cases are still not decided as quickly as required by law, and expects NSM to continue its efforts to bring case processing time for security clearance cases down to a satisfactory level in 2016.

5.4 Security interviews

In its annual report for 2014, the Committee stated that it might be necessary with an external evaluation of how security interviews are conducted. The Committee had found that the quality of the security interviews conducted varied between security clearance authorities, and that some interviews could have been conducted in a more targeted manner that was more conducive to establishing trust. Among other things, the Committee noted that the interviews often are very extensive and can take a form reminiscent of an interrogation, which can be stressful to the person concerned. Furthermore, the flexibility of the interview method has not

Photo: Erlend Aas / NTB scanpix

The NSM headquarters at Kolsås base in Bærum. Kolsåstoppen in the background.

been sufficiently utilised and adapted to each individual case. Some interviews also appeared not to be sufficiently purposeful, and any confrontations with the person concerned about his/her suitability for security clearance often came at too late a stage of the interviews. At the same time, the interviewers tend not to go deeply enough into the key issues when they are eventually brought up because the questions asked are not sufficiently open or specific.

In 2015, the Committee has been in ongoing dialogue with NSM about how security interviews should be conducted. NSM took the initiative to a meeting about the matter, where the discussion could be based on three security interviews which NSM would review in detail prior to the meeting. The Committee then selected three security interviews conducted by different security clearance authorities for review. At the meeting, NSM reviewed the purpose of security interviews, the challenges/problems it identified in the selected security interviews and what measures it wanted to implement to remedy the situation.

NSM stated that, generally speaking, the information obtained during security interviews should be relevant to the overall assessment, truthful and reliable, suited to providing a basis for assessing the reliability, loyalty and sound judgement of the person concerned, as well as to elucidating and assessing any vulnerabilities that can represent a risk in relation to the suitability of the person concerned for security clearance. Prior to the meeting, NSM had also carried out a thorough review of the selected security interviews. On the basis of this review, NSM informed the Committee of several non-conformities it had identified in the security interviews. Among other things, NSM pointed out weaknesses in the preparations, varying knowledge of the interview technique and varying degrees of suitability among the interviewers. NSM also identified weaknesses in the dynamics between the interviewers, as well as the use of closed questions and questions that were not adapted to the age and background of the person concerned. Finally, NSM pointed out that, in some interviews, information provided by the person concerned was poorly processed so that important issues were not followed up to a sufficient extent later in the interviews.

The Committee found that NSM's account of the purpose of security interviews and the challenges involved in conducting security interviews, mainly coincided with the issues the Committee had previously pointed out to NSM. Furthermore, NSM stated that, as a result of the review of the security interviews, it wanted to implement several measures to improve and further develop the security clearance authorities' expertise in this area. In that connection, NSM informed the Committee that it will make changes to the current course plan and that more courses should be organised for the security clearance authorities. These courses should also be made mandatory. Furthermore, NSM is considering whether the interviews should be conducted by professional interviewers in order to ensure that the security interviews are professionalised and that all interviewers get enough practical experience. Today, each case officer conducts the interviews with another case officer present. It would still be relevant for the case officer to participate in the interview if the practice of using professional interviewers is adopted.

During the meeting, the Committee asked questions and provided input to NSM. The Committee felt that there was a good and open dialogue about the use of security interviews.

The Committee would like to comment that no overall review of the security clearance authorities' use of security interviews has been carried out. However, the Committee is of the opinion that the review of individual security interviews carried out by the Committee and NSM, provides a good basis for making an overall assessment of the current use of security clearance interviews and for identifying several of the problems associated with the way in which the interviews are conducted. In the Committee's opinion, this is supported

34 Recommendation No 289 to the Storting (2014–2015), Chapter 2 Komiteens merknader ('The Committee's comments' – in Norwegian only).

by the fact that NSM's account raised several of the same issues as the Committee had pointed out in its reviews.

The Committee has noted that NSM has never before reviewed and evaluated its use of security interviews. It is positive that NSM has now carried out a thorough internal review of its own and certain other security clearance authorities' security interview practices. At the same time, they have used the same method for years, so it is appropriate that such a review has now been carried out.

The dialogue between NSM and the Committee has shown that it seems to be the way in which the security interviews are conducted that poses the biggest challenge to the security clearance authorities, and not the methodology on which the interviews are based. NSM has stated that the methodology allows for an adapted procedure in each individual case, but that this is contingent on good preparation, competence and implementation.

The Committee expects the strong reduction in the number of security clearance authorities in itself to result in an improvement of the quality of case processing in security clearance cases, including how security interviews are conducted.

The Committee is of the opinion that NSM takes the problems associated with security interviews pointed out by the Committee seriously, and is satisfied that NSM will implement more measures in this area in the time ahead. This should raise the competence of both NSM and the other security clearance authorities in relation to how they should conduct security clearance interviews. The Committee will follow this work closely and carry out oversight activities in relation to more security interviews in the course of 2016.

On the basis of the Committee's dialogue with NSM and the measures that will be implemented, the Committee does not find it necessary at the present time with an external evaluation of how security interviews are conducted.

5.5 Oversight of positive security clearance decisions in cases where the person concerned has foreign closely related persons

5.5.1 Introduction

In connection with one of the inspections of NSM in 2014, the Committee requested five security clearance cases with positive outcomes in which the initial decision had been made by NSM and by the Ministry of Foreign Affairs, respectively. Common to all these cases is that closely related persons of the person concerned were citizens of countries with which Norway has no security cooperation. In particular, the Committee's oversight of positive decisions in security clearance cases aims to find out whether similar cases are treated in the same way in order to avoid unjustified differential treatment by the same security clearance authority or by different security clearance authorities.

Based on a review of the cases, the Committee had some questions and remarks relating to the case processing.

5.5.2 Positive decisions made by NSM

General information

Among other things, the Committee found that several of the submitted case files lacked minutes and recordings of the security interviews, and remarked that it is necessary for oversight purposes that all files are complete. Furthermore, the Committee pointed out that the content of some internal grounds drawn up at the same time and some assessments made following the security interviews were somewhat brief.

A brief description of the Committee's remarks concerning some of the cases

In one of the cases, NSM cleared the person concerned for the highest security clearance level, COSMIC TOP SECRET (CTS), without considering the significance of the lack of personal history information about many of the person's siblings. Their connection was to a country with which Norway has no security cooperation.

The Committee questioned NSM assessments in this case from an equal treatment perspective, considering that in similar cases, the person concerned is often denied security clearance solely on the basis of insufficient information about the personal history of closely related persons. NSM referred to the fact that security interviews had been conducted in the case and that the person concerned's connection to the family in the country in question was a key topic in both interviews. NSM therefore believed that the case had been sufficiently elucidated, even though it acknowledged that the personal history requirement could have been considered more closely.

In its concluding letter to NSM, the Committee referred to its remarks in *Complaint case 3*, see section 5.6.3, where NSM states that the insufficient personal history for the person in question's spouse alone gave grounds for denying security clearance pursuant to the Security Act Section 21 first paragraph letter j concerning lack of opportunity to carry out satisfactory vetting. The Committee therefore found it difficult to see that a specific and individual overall assessment can be made of the person concerned's suitability for security clearance when there is insufficient information about the personal history of other closely related persons, but not about the person's spouse/cohabitant/partner. The Committee remarked in relation to NSM that such a practice will entail differential treatment in security clearance cases.

In another case with a positive outcome, the person concerned was cleared for CTS without a security interview being conducted, despite the fact that the person had a connection to a country with which Norway has no security cooperation. The Committee could not find any documentation in the case to show that an assessment had been made of how important the country is to Norway from a security perspective.

In its concluding letter to NSM, the Committee again referred to its remarks in *Complaint case 3*, see section 5.6.3. The person the positive security clearance decision concerned had a connection to, and closely related persons who were citizens of, the same country as the closely related persons of the person the complaint case concerned. In connection with the correspondence in the complaint case, NSM was of the opinion that insufficient personal history from the country in question constituted grounds for automatically denying security clearance on grounds of insufficient information about the personal history of closely related persons, without a specific and individual overall assessment being made of the suitability of the person concerned.

In response to the Committee sending parts of the annual report to NSM to check for classified information, errors and misunderstandings relating to factual information, NSM commented on the facts relating to the Committee's concluding statement in the case in a letter of 26 February 2016. The Committee will reply to NSM's letter.

5.5.3 Positive decisions made by the Ministry of Foreign Affairs

The Committee could not find that the internal grounds drawn up at the same time showed that a specific and individual overall assessment had been made of the suitability of the person concerned for security clearance, including an assessment of the person's connection to other states.

Nor was it documented whether the Ministry had considered the fact that the person's closely related persons did not meet the requirement for ten years' personal history to begin with. The Committee stated the following about the necessity of conducting safety interviews:

> 'The fact that closely related persons of the person concerned come from a country with which Norway has no security cooperation, and that the related persons do not meet the requirement for ten years' personal history to begin with, indicates, in the Committee's opinion, that it is not "clearly unnecessary" to conduct a security interview with the person concerned, cf. the Security Act Section 21 third paragraph.'

The Ministry of Foreign Affairs stated that it mostly shared the Committee's points of view on the assessment of the cases in question, and that its practice had been adjusted accordingly.

5.5.4 Conclusion

During its many years of overseeing security clearance cases, the Committee has seen several fundamental problems with cases in which the persons concerned or their closely related persons have a connection to a foreign country. The issues relate to some of the Committee's key points for oversight: equal treatment, compliance with important case processing rules, the importance of country assessments, personal history and observation periods. On this basis, the Committee has decided to initiate a project in 2016 to systematically review a large number of such cases.

5.6 Complaint cases considered by the Committee

5.6.1 Introduction

The Committee received six complaints against NSM in 2015. On the basis of the complexity and scope of the cases, the Committee has used a great deal of resources on these complaint cases. A decision in a security clearance case is often of decisive importance to a person's future career. It is therefore essential that these cases are considered by the security clearance authorities in a fair manner that safeguards due process protection. In cases resulting in criticism, the complainant can also in many cases be informed of the grounds for the Committee's conclusion.

Of the cases the Committee concluded in 2015, the following four cases gave grounds for critical remarks from the Committee:

5.6.2 Complaint cases 1 and 2 – long case processing time

In its annual report for 2014, section 5.8 – Complaint case 3, the Committee discussed a complaint case where NSM was criticised for its long processing time in a security clearance case. In 2015, the Committee received another complaint in the case, and NSM was again criticised for its long case processing time, as it has had the case under consideration for approximately three years. The Committee stated the following in its concluding letter to NSM, of which the complainant was informed:

> 'The Committee notes that NSM has now had the security clearance case under consideration for approximately three years in total. In the above-mentioned letter, NSM writes that the security clearance case will be forwarded to the Ministry of Defence for consideration of the appeal.
>
> The Committee is of the opinion that NSM's case processing time has been unreasonably long, both for the consideration of case on its merits and the question of document access.'

In another complaint case, the Committee criticised NSM for its long case processing time in a security clearance case. The Committee criticised NSM for having taken two years and three months to complete the consideration of the appeal against its initial refusal to grant security clearance. The Committee was later informed that NSM had failed to keep its promise to the Committee to conclude the case, so that a further four months elapsed before NSM forwarded it to the Ministry of Defence as the appellate body.

5.6.3 Complaint case 3 – insufficient information about the personal history of closely related persons

In the annual report for 2014 section 4.8 – Complaint case 4, the Committee wrote that the person concerned was granted NO CLEARANCE after marrying a foreign partner of the past eleven years. In the Committee's opinion, the NO CLEARANCE decision was not to a sufficient extent based on an individual assessment of whether the person concerned was fit to hold security clearance, as required by the Security Act Section 21.

On the basis of the circumstances in the case, the Committee believed that it should be possible for NSM to carry out a specific and individual overall assessment of whether the person concerned is fit to process sensitive information. Furthermore, NSM could have conducted a security interview with the person concerned. On this basis, the Committee requested that NSM reconsider the security clearance case in question and inform the Committee about the outcome. Five months after the Committee's concluding statement, NSM informed the Committee that it would not reconsider the security clearance case. Among other things, NSM pointed out that the person concerned lost the security clearance because of a requirement relating to the personal history of spouses that follows from the Personnel Regulations Section 3-7 first paragraph, which the person's spouse failed to meet. NSM wrote:

> 'One of the most basic preconditions for being able to assess a person's suitability for security clearance is that it must be possible to obtain security-relevant information about the person concerned and any closely related persons covered by the vetting process. NSM finds that marriage or cohabitation will always entail a certain risk that the spouse or cohabitant could influence a person with security clearance to act in a manner contrary to security interests.'

NSM claimed that insufficient information about the personal history of a closely related person alone gave grounds for denying security clearance in the case in question. Only once the complainant's spouse has obtained the personal history that NSM deems necessary will NSM make an overall assessment of the complainant's connection to the country in question in connection with the assessment of the suitability of the person concerned.

In its concluding letter to NSM, the Committee remarked that the purpose of security clearance is to determine whether the person concerned is fit to process sensitive information. The security clearance authority shall endeavour to clarify whether there are circumstances relating to the person concerned that could be used as a means of exerting pressure on him/her – to identify any vulnerabilities. To determine a person's suitability for security clearance, 'decisions regarding clearance shall be based on a case-by-case overall evaluation of the available information',[35] where insufficient information about the personal history of closely related persons will be one of the elements to which importance must be attached. The Committee stated:

> 'In the Committee's opinion, the personal history requirement set out in the Security Act Section 21 first paragraph cannot be regarded as a form of precondition for carrying out a specific and individual overall assessment of the suitability of the person concerned, as NSM seems to interpret the provision. The Committee cannot see that the regulations allow for insufficient information about the personal history of a spouse/cohabitant/partner in itself to form grounds for a negative security clearance decision pursuant to the Security Act Section 21 first paragraph letter j, without a specific and individual overall assessment being made of the *suitability of the person being vetted with respect to security,* cf. the third paragraph of the provision.
>
> This understanding of the wording of the Act is supported by the practice that the Committee has seen in certain other security clearance cases. The Committee has made

a note of cases in which the security clearance authorities, including NSM, have in practice carried out a specific and overall assessment of whether the person concerned is fit to hold security clearance, despite of there being insufficient information about the personal history of closely related persons covered by the vetting, which, in principle, makes it impossible to carry out satisfactory vetting, cf. the Security Act Section 21 first paragraph letter j, the Regulations concerning Personnel Security Section 3-7, and NSM's circular. The Committee therefore finds it difficult to see that a specific and individual overall assessment can be made of the person concerned's suitability for security clearance when there is insufficient information about the personal history of other closely related persons, but not about the person's spouse/cohabitant/partner.'

The Committee also remarked that a security interview can be used to clarify any doubts about the suitability of the person concerned, including security-relevant matters relating to closely related persons. Among other things, the Committee referred to NSM's practice in other cases, where clearance for the highest security clearance level (CTS) was granted *without a security interview being conducted*. This was done despite the fact that the person concerned had dual citizenship and had a connection to the same country that the complaint case in question concerns. In conclusion, the Committee stated:

'The Committee is still of the opinion that NSM should carry out a specific and individual overall assessment of whether [the complainant] is fit to hold clearance for the SECRET level, and that it should conduct a security interview with [the complainant] to clarify [the complainant's] suitability for security clearance. That would better safeguard [the complainant's] due process protection.

The Committee is of the opinion that confidence in the security clearance system could be weakened if the security clearance authorities assess the necessity of complying with the statutory requirement for a specific and individual overall assessment in security clearance cases solely on the basis of the personal history of closely related persons and their connection to the person concerned. If a specific and individual assessment is made in some cases of this type, but not in others, the consideration of these security clearance cases will be perceived as somewhat random. This gives cause for concern about due process protection.

The Committee noted that NSM would not reconsider the case, but pointed out that there was justified and significant doubt about whether the consideration of the case complied with the Security Act Section 21.

In response to the Committee sending parts of the annual report to NSM to check for classified information, errors and misunderstandings relating to factual information, NSM commented on the facts relating to the Committee's concluding statement in the case in a letter of 26 February 2016. The Committee will reply to NSM's letter.

5.6.4 Complaint case 4 – Change in disfavour of the complainant, inadequate follow-up of granted access, the requirement for grounds to be given, and long processing time

On the basis of a complaint, the Committee criticised certain aspects of NSM's case processing in a security clearance case where it made the initial decision. The Committee criticised NSM for expanding what is known as the 'observation period' when it prepared the case for consideration by the appellate body. The observation period is the time that must elapse before the person concerned can have his/her clearance status reconsidered. The subordinate body (NSM) changed the case in disfavour of the complainant. This is in violation of the Public Administration Act Section 33, which applies in security clearance cases. The Committee also criticised NSM for inadequate follow-up of access granted to the case documents, so that, in practice, access was not given. The Committee also pointed out that the grounds for the negative decision were unclear. The Committee stated that a decision to deny security clearance is so invasive that it strengthens the requirement that the grounds given must be sufficiently precisely and clearly worded, so that they reflect the considerations that have been decisive in the case. Finally, NSM was criticised for its long case processing time.

The Committee is of the opinion that the requirements for good administrative practice are very important in administration processes which are partly exempt from public access, a category which security clearance cases still fall into. The fact that the security clearance authority can restrict access to information about parts of the process on the basis of security considerations may be a burden to the person being considered for security clearance. This should cause the security authority to exercise its authority in a considerate manner.

The appellate body found partly in favour of the complainant, who was granted clearance for a lower level than requested. The Committee found no basis for criticising the appellate body's (the Ministry of Defence) consideration of the case.

35 Cf. the Security Act Section 21 first paragraph first sentence.

6.
The Norwegian Defence Security Agency (FSA)

Photo: Forsvaret

6.1 General information about the oversight

The Committee conducted three inspections of the FSA in 2015.

The FSA's processing of security clearance cases is particularly important in the Committee's oversight of the agency. The FSA is the country's largest security clearance authority by far and decides approximately 17,000 cases each year. The FSA has around 3,000 security clearance cases under consideration at all times. The Committee reviews all negative security clearance decisions made by the FSA that have not been appealed, as well as appealed security clearance cases where the agency granted the appeal in part or in full.

The Committee also oversees the FSA's protective security activities, and, in that connection, carries out spot checks of investigations into activities that represent a threat to security targeting the Armed Forces (security investigations) and operational cases that are part of the agency's responsibility for military counterintelligence (Mil CI) in Norway in peacetime. One of the Committee's primary duties in this connection is to oversee the FSA's processing of personal data as part of its protective security activities.

The Committee has been kept up to date on the regulatory situation in relation to the FSA's performance of its duties. In the annual report for 2013, the Committee reported that it would keep up to date on the preparation of a cooperation agreement between PST and the FSA. The agreement has still not been signed.

The Committee received two complaints against the FSA in 2015. One complaint concerned a refusal to grant authorisation for RESTRICTED. The complaint case was concluded without criticism of the FSA. The other complaint concerned long case processing time and resulted in criticism of the agency.

Following dialogue with the Committee about how security interviews are conducted, the agency has appointed a working group to look into an evaluation method for security interviews.

6.2 Case processing time for security clearance cases

In 2015, the FSA stated that the case processing time has been too long, and that this could have a negative effect on the Armed Forces' operational capabilities. At the beginning of 2015, the FSA informed the Committee that the agency's case processing capacity was insufficient in relation to its duties. The need for additional resources had been reported to the Ministry of Defence. In the same period, the number of security clearance cases under consideration by the FSA increased due to the agency's insufficient case processing capacity. In addition, there was an increase in the number of appeals against negative security clearance decisions. The FSA received additional case processing resources in 2015, and, at year end, the agency was processing more security clearance cases than it was receiving. The Committee has been informed that the FSA will receive further resources in 2016.

The FSA has informed the Committee about measures implemented to improve the situation. The agency has established a new section under the office for personnel security tasked with, among other things, handling complaint cases and helping to reduce case processing time, as well as handling the FSA's contact with the EOS Committee. Furthermore, the FSA has initiated a pilot project related to security clearance of national service personnel. The objective of the pilot project is to clear all personnel before they start their military service. The Committee will maintain focus on the FSA's case processing time in the time ahead.

The FSA regularly provides the Committee with an overview of, among other things, the total number of requests for security clearance, negative security clearance decisions broken down by different fields, concluded cases, cases dropped and the number of complaint cases etc. During the Committee's inspection in October 2015, the Committee noted that as much as 83.7 per cent of cases involving negative findings relating to the financial situation of the person concerned resulted in the request for security clearance being denied. This was mostly due to the persons concerned failing to return the authorisation to obtain further information or provide statements regarding the findings. This means that the reason for the denials were not the financial situation of the persons concerned, but inadequate follow-up on their part. The FSA stated that this shows that the security clearance authorities need access to more sources in its vetting of personnel.

6.3 Processing of personal data in the FSA's database for operational activities

The Committee's oversight of the processing of personal data in the FSA have been discussed in, among other things, the annual reports for 2010,[36] 2011[37] and 2012.[38]

36 Chapter V section 3.

37 Chapter VI section 4.

38 Chapter VI section 6.

During an inspection in 2014, the FSA, on the Committee's request, presented paper transcripts of some registrations of persons from an operational database. The FSA stated that several of the entries had been deleted from the database the day before the inspection. The data therefore only existed in the paper copy presented and later sent to the Committee.

The Committee requested that the FSA explain the grounds for processing the personal data of several persons in the database. The documents were returned to the agency together with a letter in which the Committee asked questions.

In its reply, the FSA stated that the agency was unable to explain the grounds for processing the personal data of several of the persons registered because they had shredded some of the paper transcripts.

The Committee concluded as follows in its concluding letter to the FSA concerning the agency's shredding of documents:

> 'By way of introduction, the Committee would like to remark that it expects the FSA to be capable of answering the Committee's questions asked on the basis of documents sent to the Committee for review, even if electronically stored data etc. are deleted in the meantime in accordance with the regulations concerning the processing of data in the FSA. It is clearly unfortunate that the FSA shredded these documents, thereby rendering itself incapable of giving adequate answers to the Committee's questions. *The Committee assumes that the FSA believes that there was (no longer) a basis for continuing the processing of the data that were shredded/electronically deleted.'*

The FSA also stated that the database in question would be closed down in 2015. At the beginning of January 2016, however, the database was found to still be active, and the FSA is still processing personal data regarding many persons in this database, despite the fact that the data are no longer required for the purpose of the processing.[39] This also included the personal data of persons the FSA said had been deleted from the database. This is unfortunate.

As regards the FSA's grounds for processing the personal data in question in the database, the Committee noted that it *seemed doubtful whether the FSA had a sufficient legal basis for registering several of the persons in question at all.*

39 Cf. the Instructions for Defence Security Service Section 20 first paragraph letter c.

7.
The Norwegian Intelligence Service (NIS)

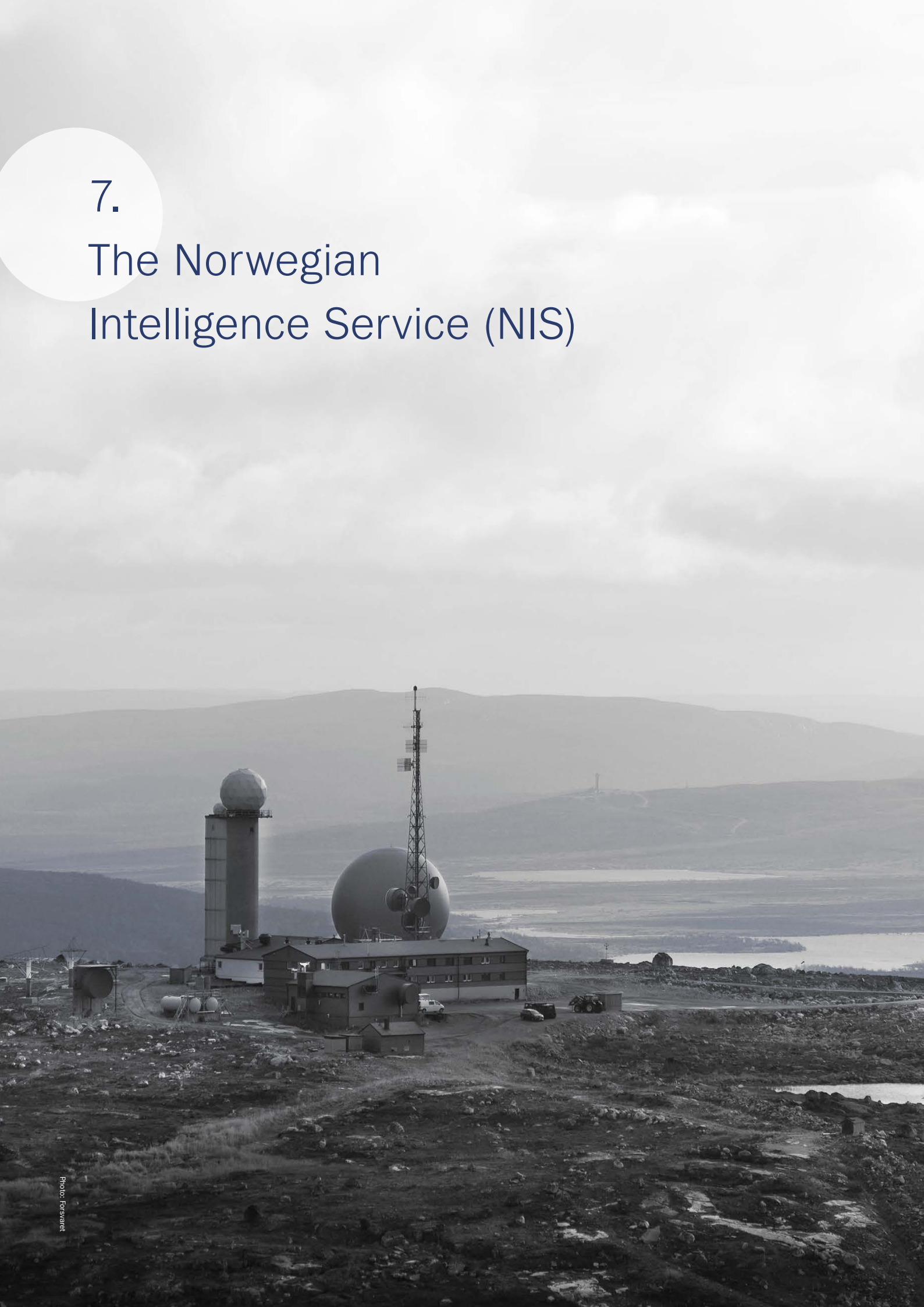


Photo: Forsvaret

7.1 General information about the oversight

The Committee conducted four inspection of the NIS headquarters in 2015, in addition to one inspection of a local station, the Norwegian Armed Forces' station in Ringerike.

The Committee shall ensure that NIS's activities are carried out within the framework of the service's established responsibilities, and that no injustice is done to any person, cf. the Directive relating to Oversight of Intelligence, Surveillance and Security Service Section 11 subsection 1 letter a. In its inspection of NIS, the Committee oversees the following:

- The service's technical information collection
- The service's exchange of information with cooperating domestic and foreign services
- The service's computer systems
- Cases submitted to the Ministry of Defence and internal approval cases.[40]

During the inspections, the Committee is regularly briefed about NIS's ongoing activities, including the service's cooperation cases with other EOS services, the threat situation and cases submitted to the Ministry of Defence, as well as internal approvals. Such approvals can authorise surveillance or disclosure of information about Norwegian legal persons to foreign partners. For example, such approvals can give NIS internal authorisation to monitor a Norwegian national's communication equipment when the person is abroad. The legislation does not require external permission from the courts in such cases in the way it does for PST in relation to e.g. communications control.

In its oversight of NIS, the Committee focuses in particular on ensuring that the service does not violate the statutory prohibition against monitoring or in any other covert manner procuring information concerning Norwegian physical or legal persons on Norwegian territory, cf. the Intelligence Service Act Section 4 first paragraph.

The legal position of Norwegian legal persons abroad is not regulated by the Intelligence Service Act, but the service is nonetheless obliged to respect the rights set out in the European Convention on Human Rights (ECHR), including Article 8 concerning the right to respect for private and family life. In 2013, the Ministry of Defence adopted provisions regarding collection of information concerning Norwegian persons outside Norwegian territory.[41] In order for NIS to be allowed to monitor or in any other covert manner procure information concerning Norwegian persons abroad, three defined conditions must be met. Firstly, the collection of information must take place as part of NIS's performance of its statutory duties. Secondly, the information concerned must be information that NIS can lawfully hold pursuant to the Intelligence Service Act Section 4 second paragraph.[42] Thirdly and finally, the collection must be deemed to be necessary following a proportionality assessment where account is taken of the need to safeguard important national interests and the consequences for the person about whom information is collected. This is also an important focus for the Committee's oversight.

Photo: Forsvaret

The NIS headquarters at Lutvann.

In 2015, NIS declassified its presence at the Norwegian Armed Forces' Ringerike station at Eggemoen near Hønefoss. The station was established in 2000 and staffed from 2005. NIS collects information from selected satellites in space from this station. The Committee conducted inspections of NIS's activities at Eggemoen in 2006, 2009 and 2012 without being able to mention this in its unclassified annual reports. None of the inspections mentioned resulted in criticism or other follow-up in relation to the service. Nor did the 2015 inspection of the station.

On 2 December 214, the service adopted *Instructions relating to facilitation of EOS inspections and the handling of enquiries from the EOS Committee*. This is the first time the Committee has seen such instructions in the EOS services. This is a positive development.

7.2 Special report concerning the legal basis for NIS's surveillance activities

In 2016, the EOS Committee will submit a special report to the Storting concerning the legal basis for NIS's surveillance activities. The background to this report is the need to evaluate whether the Intelligence Service Act provides an adequate legal basis for NIS's surveillance activities seen in light of technological and legal developments, as well as the development of the threat situation.

7.3 The Committee's right of inspection of NIS

An extensive account of the Committee's right of inspection of NIS was provided in the annual report for 2013. The case is based on the Storting's plenary decision from 1999 stating that a special procedure shall apply for disputes about access to NIS documents. The decision did not lead to any amendments being made to the Act or Directive governing the Committee's oversight activities.[43] The Storting's 1999 decision was based on the particular sensitivity associated with NIS's sources, the identity of persons with roles in occupation preparedness and particularly sensitive information

received from cooperating foreign services. The Storting's Standing Committee on Scrutiny and Constitutional Affairs will await the evaluation of the EOS Committee before deciding whether the Committee's right of inspection shall apply in full also in relation to NIS.[44] In practice, the plenary decision from 1999 means that the Committee is not granted access to information that the service deems to be 'particularly sensitive'. In 2013, NIS prepared an abbreviated, unclassified definition of 'particularly sensitive information'. In 2015, the Ministry of Defence decided to declassify the whole definition of this concept. The declassified definition is as follows:

1. The identity of the human intelligence sources of NIS and its foreign partners
2. The identity of foreign partners' specially protected civil servants
3. Persons with roles in and operational plans for occupational preparedness
4. NIS's and/or foreign partners' particularly sensitive intelligence operations abroad* which, if they were to be compromised,
   a. could seriously damage the relationship with a foreign power due to the political risk involved in the operation, or
   b. could lead to serious injury to or loss of life of own personnel or third parties.

*By 'intelligence operations abroad' is meant operations targeting foreign parties (foreign states, organisations or individuals), including activities relating to such operations that are prepared and carried out on Norwegian territory.

The Committee is regularly informed about the number of cases and amount of data exempted from the Committee's right of inspection, as well as which of the four categories of the above-mentioned definition the case falls into. In 2015, NIS adopted *Guidelines for the processing of particularly sensitive information.* Among other things, the guidelines state that if information can no longer be regarded as particularly sensitive information, it shall no longer be categorised as such and shall be made available for the Committee's oversight. Such decategorisation shall be considered once an operation has been concluded and subsequently at regular intervals. So far, no such decategorisation has taken place.

In previous annual reports, the Committee has described the dialogue between the Committee and the service as regards facilitation of access, which in 2014 led to the Committee being authorised to conduct free searches in the service's computer systems, with the exception of information categorised as particularly sensitive, see above. In 2015, NIS has further improved and facilitated the Committee's independent searches. The solution is satisfactory.

7.4 Non-conformity reports relating to NIS's technical information collection

NIS has introduced a procedure for reporting to the Committee any non-conformities that the service identifies in its technical collection system. None of the non-conformities identified in 2015 resulted in the collection of information about individuals. NIS has informed the Committee that each non-conformity has been followed up by improvement of internal procedures to prevent human errors, as well as by improvements to the technical systems.

The Committee has found no reason to follow up the non-conformities identified in 2015. In the Committee's opinion, NIS's reporting and follow-up shows a willingness and ability to safeguard fundamental due process protection guarantees, and also shows that the service follows up the requirement to keep the Committee up to date about circumstances of relevance to the oversight.

7.5 NIS's procedures for deleting operational information

In the annual report for 2014, the Committee described the questions it had asked NIS concerning the service's procedures for deleting information processed in the course of the service's operational activities. On the basis of the correspondence with the Committee, the service stated that it would consider drawing up general rules for the deletion of operational information, particularly information about Norwegian physical and legal persons. In 2015, NIS informed the Committee that work has been initiated internally to prepare comprehensive and general internal regulations for the service's processing of personal data. The service stated that in the long term, it is desirable to establish general public regulations for the service's processing of personal data. ***The Committee will keep informed about the service's work in this area.***

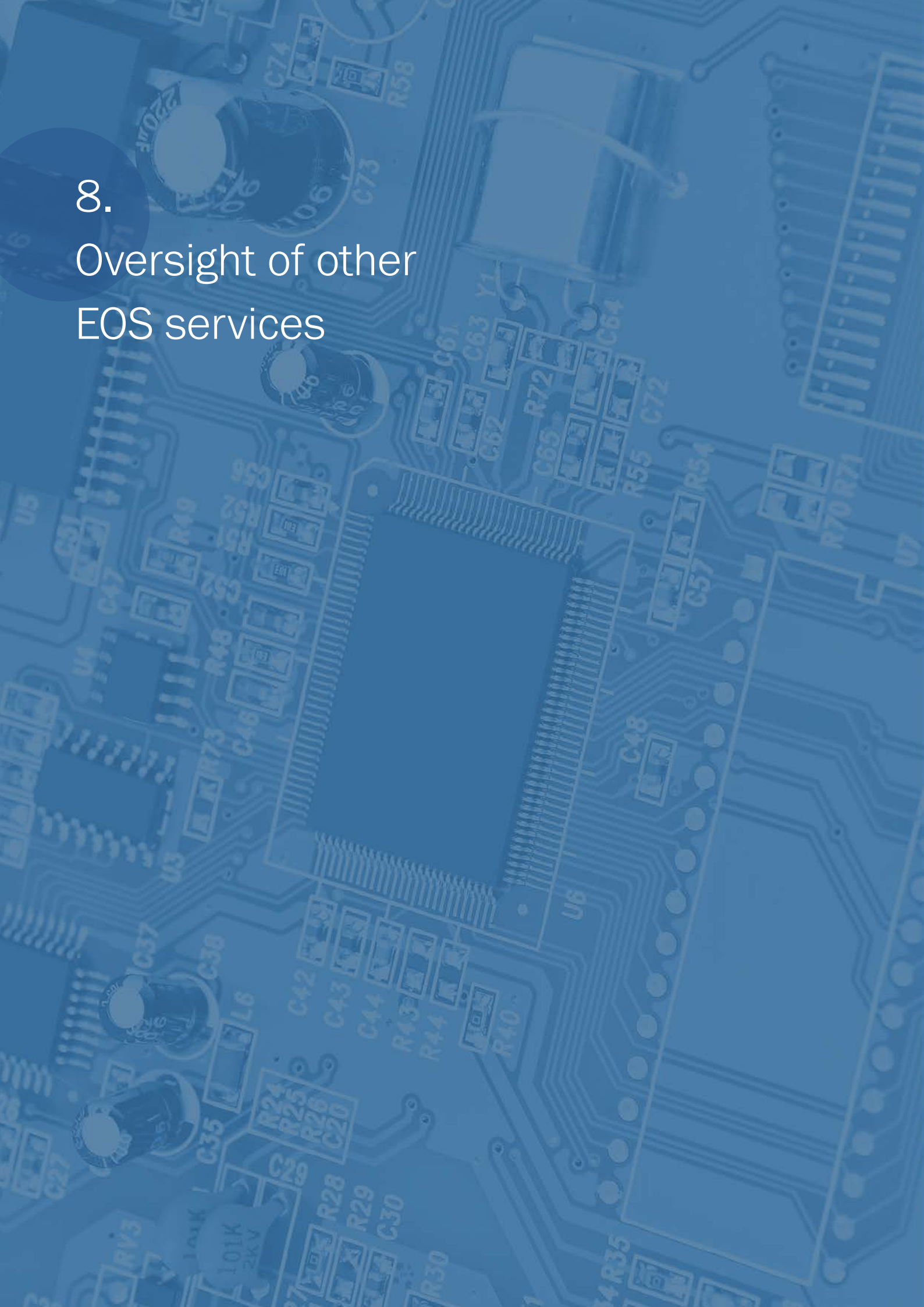
40 Cf. the Royal Decree of 31 August 2001 No 1012 relating to instructions for the Norwegian Intelligence Service Section 13 letter d stating that 'matters of particular importance or that raise questions of principle' shall be submitted to the Ministry of Defence for consideration.

41 Supplementary provisions concerning the Norwegian Intelligence Service's collection of information relating to Norwegian persons abroad and the disclosure of personal data to cooperating foreign services. Adopted by the Ministry of Defence on 24 June 2013 pursuant to the Instructions for the Norwegian Intelligence Service Section 17. The instructions can be found in the Lovdata database.

42 The Intelligence Service Act Section 4 second paragraph states that NIS may 'only hold information concerning Norwegian physical or legal persons when such information is directly associated with the duties of the Norwegian Intelligence Service pursuant to Section 3 or is directly associated with such persons' work or assignments for the Norwegian Intelligence Service.'

43 See Document No 16 (1998–1999), Recommendation No 232 to the Storting (1998–1999) and minutes and decisions by the Storting from 15 June 1999.

44 See Recommendation No 289 to the Storting (2014–2015), Chapter 2 Komiteens merknader ('the Committee's comments' – in Norwegian only).



8. Oversight of other EOS services

8.1 General information about the oversight

The Committee continuously oversees intelligence, surveillance and security service carried out by, under the control of or on the authority of public authorities.[45] In other words, the oversight area is not linked to particular organisational entities, but is defined by function.

Pursuant to the Directive relating to Oversight of Intelligence, Surveillance and Security Service Section 11 subsection 2 letter e, the Committee shall carry out annual inspections of at least two Intelligence Service units and/or intelligence/security service at military units, and of the personnel security service of at least two ministries/government agencies.

In 2015, the Committee inspected the intelligence and security services of the Naval Special Operations Force. The Committee also inspected the personnel security service of the Norwegian Communications Authority (Nkom) and the Ministry of Defence. The inspection of Nkom also included investigation activities relating to allegations of fake base stations for cell phones in Oslo city centre, see section 2.2.2.

The above-mentioned inspections were prepared in advance by the Committee Secretariat, among other things by searches in computer systems. The Committee was given access to FISBasis as requested, cf. section 8.2. Neither the inspection of the Naval Special Operations Force nor the inspection of Nkom gave grounds for follow-up or criticism.

On the basis of the inspection of the Ministry of Defence's personnel security service, the Committee criticised the Ministry for very long case processing time in two cases. In both cases, it took the Ministry, as the appellate body, around 2.5 years to reach a decision. That is far too long. The Ministry of Defence has informed the Committee that the Ministry's security clearance authority has been strengthened. The average case processing time for all appeal cases decided by the Ministry of Defence in 2015 was 245 days. Based on the figures that the Committee requested, the Committee noted that the Ministry's backlog of security clearance cases and appeals has decreased by 82 per cent in 2015.

In 2015, the Committee received one complaint against the personnel security service of the Ministry of Defence on grounds of its long case processing time. The Committee criticised the Ministry for allowing more than four months to pass before the case was registered in the case processing system so that the vetting process could commence, and expressed an expectation for the security clearance authority to prioritise the case.

In a complaint case against NSM, cf. section 6.5.2. – *Complaint case 1*, the Ministry of Defence was criticised for long case processing time. The Committee endorsed the Ministry of Defence's assessment that the Ministry should have completed the processing of the complaint concerning inadequate access to documents in the security clearance case sooner.

8.2 The Committee's access to FISBasis

In its annual reports for 2012, 2013 and 2014, the Committee reported that it has not had sufficient de facto access to the Norwegian Armed Forces' FISBasis systems, and that, as a result of inadequate progress in the case, it had contacted the Chief of Defence and requested that the matter of the Committee's user access be clarified immediately. In 2015, the Norwegian Armed Forces' Cyber Defence has prepared a procedure that describes how the Committee shall be guaranteed access to the systems in connection with announced as well as unannounced inspections. In connection with the announced inspection of the Naval Special Operations Force in 2015, the Committee was given access as requested. ***The Committee is satisfied with the established procedure.***

45 Cf. the Oversight Act Section 1 first paragraph.

9.
External relations and administrative matters

9.1 The Committee's external relations

The EOS Committee is in contact with relevant external environments. The Committee's network of external contacts include other countries' oversight bodies, research communities in Norway and abroad, other national oversight bodies, and the media and society at large. The Committee wants transparency regarding its work.

Changes in the international threat situation result in increasing internationalisation of the services' work. The increased international collaboration between services brings new challenges for the oversight bodies. The EOS Committee monitors this development and is working to improve collaboration with other countries' oversight bodies, among other things through exchange of experience and mutual visits. Contact with oversight bodies in other countries is very useful because the exchange of experience of professional and organisational issues stimulates innovative thinking and improvement of the Committee's work methods.

The Committee also wishes to share its own experience in order to help to raise competence and develop institutions in other countries, both in its dealings with 'young democracies' and in relation to established democratic states. In the past year, the Committee and the Committee Secretariat have been in contact with members of parliament and oversight bodies from the Caucasus, the Western Balkans, Ukraine, Germany, Austria, Sweden, the Netherlands and Switzerland, among others. The Committee has also participated in meetings in the European Parliament where increased collaboration between European oversight bodies was on the agenda. The Committee also met with the Council of Europe Commissioner for Human Rights. In the meeting the Committee provided input to the Commissioner's report on democratic and efficient oversight of European security services. Furthermore, the Committee has been involved in relevant research collaboration that could strengthen the democratic oversight of secret services also outside Norway's borders.

Representatives of the Committee and the Committee Secretariat have attended a wide range of events in 2015. Whether participating in debates and seminars or hosting visitors from abroad, the Committee has endeavoured to be open and active in issues relating to oversight of the secret services. An overview of external contact is provided in appendix 2.

9.2 Administrative matters

The Committee's expenses amounted to NOK 12,499,000 in 2015, compared with a budget of NOK 13,506,000, including transferred funds. The Committee has applied for permission to transfer the unused portion of its allocations to the budget for 2016. The main reason for the Committee's underspending is that it took longer than expected to fill two of the three newly created positions, along with reimbursements from the Norwegian Labour Administration (NAV) for two short-term leaves of absence where no temporary substitutes were used.

The Committee Secretariat is now using all the offices in the Committee's premises. The Committee needs to find bigger premises. It is also assumed that it may become relevant to expand the secretariat staff. The Committee has begun the processes of defining requirements for its new premises, and will contact the Storting regarding this matter during the first half of 2016. This enquiry will also include any needs for follow-up of the Evaluation Committee's report.[46]

46 Document 16 (2015–2016) Report to the Storting from the Evaluation Committee for the Norwegian Parliamentary Intelligence Oversight Committee (EOS Committee).

10. Proposals for amendments of laws and regulations

10.1 Deferred access

Most of the Committee's correspondence is with the EOS services and is protected for security reasons, and is therefore classified under the Security Act Section 11. The unclassified part of the Committee's correspondence with public authorities falls under the scope of the Freedom of Information Act's[47] provisions on access when it is received by the public authority with which the Committee is corresponding. In cases where this correspondence is part of the Committee's preparation of a case that is under consideration for submission to the Storting as part of the constitutional oversight, the Committee has found that it may be necessary for information about a case not to be made public until the case has been received by the Storting, see the Auditor General Act[49] Section 18 second paragraph and the Freedom of Information Act Section 5.

The Auditor General Act Section 18 second paragraph reads as follows:

> 'Case documents that are prepared by or for the Office of the Auditor General in cases that are under consideration for submission to the Storting as part of the constitutional oversight shall not be made public until the case has been received by the Storting. The Office of the Auditor General will notify the relevant government agency that the case is of such a nature. If such a case is closed without any submission to the Storting, it will become public when the Office of the Auditor General has notified the government agency in question that the case has been closed.'

The Freedom of Information Act Section 5 second paragraph concerning deferred access reads as follows:

> 'For case documents drawn up by or for the Office of the Auditor General in cases that the said Office is considering presenting to the Storting as part of the exercise of constitutional oversight, access will not be given until the case has been received by the Storting or when the Office of the Auditor General has notified the administrative agency concerned of the conclusion of the handling of the case, see Section 18 second paragraph of the Act of 7 May 2004 No 21 relating to the Office of the Auditor General.'

The Committee asks the Storting to consider enshrining in law a similar rule concerning deferred access for the EOS Committee. The Committee has not objected to access being given to the Committee's unclassified correspondence with public authorities in 2015.

47 Cf. Act No 16 of 19 May 2006 relating to the right of access to documents held by public authorities and public undertakings (the Freedom of Information Act).

48 Act No 21 of 7 May 2004 relating to the Office of the Auditor General.

11. APPENDICES

Appendix 1 – Definitions

Authorisation
Decision to grant a person with security clearance access to information with a specified security classification.

Averting investigation
Investigation for the purpose of preventing a criminal act from being committed.

Classified information
Information that shall be protected for security reasons pursuant to the provisions of the Security Act. This information shall be marked with a security classification, for example CONFIDENTIAL.

Computer script
A script is a computer program that is designed to e.g. automatically identify registrations that are ready for a manual review in accordance with the five-year rule.

Covert coercive measures
Investigation methods whose use the suspect is unaware of, for example communications control, covert audio surveillance and secret searches.

CTG
The Counter Terrorism Group (CTG) is a European forum for counter terrorism collaboration between the security services of the EU states, Norway and Switzerland.

DocuLive
An archive and case processing system.

Drop a case
Decide that a case will be concluded without a decision being made based on the merits of the case.

Folder structure
Windows Explorer can be used to view the folder structure of a hard disk/network station, including all files processed there, for example the I area.

Information processing
Any form of electronic or manual processing of information.

Intelligence register
Register of intelligence information that is deemed necessary and relevant for PST in the performance of its duties. PST uses the intelligence register Smart.

Intelligence registration
Processing of information that is deemed necessary and relevant for PST in the performance of its duties, and that does not warrant opening of or processing in a prevention case.

Investigation case
Case opened for the purpose of investigating whether a criminal offence that falls within PST's area of responsibility has taken place.

Mimir
Case processing tool used in security clearance cases.

Observation period
Decision regarding when a request for a person to be granted security clearance may be resubmitted.

PEACE model
Police investigative interview technique. Security interviews are based on a version of the PEACE model that has been adapted for use in security interviews.

Personal data
Information or assessments that can be linked to an individual.

Personnel security
Measures, actions and assessments made to prevent persons who could constitute a security risk from being placed in a situation that makes the risk more immediate.

Prevention case
Case opened for the purpose of investigating whether someone is preparing to commit a criminal offence that PST is tasked with preventing.

Requesting authority
A body that, as or on behalf of an authorising authority, requests vetting of personnel

Restriction of access to information
Marking of registered information for the purpose of limiting future processing of the information in question, cf. the Police Register Act Section 2 subsection 10.

Security clearance
Decision made by a security clearance authority regarding a person's presumed suitability for a specified security classification.

Security clearance authority
Public body authorised to decide whether or not people should be granted security clearance.

Security clearance case
Case concerning a decision to grant or deny security clearance, requires an assessment of the person's suitability.

Security interview
Interview conducted by the security clearance authority in order to assess a person's suitability in a security clearance case.

SIS
Schengen Information System (SIS).

Smart
PST's intelligence register.

Smartsak
PST's tool for prevention cases and investigation cases.

The five-year rule
The requirement for PST's intelligence registrations to be re-evaluated if no new information has been added during the past five years.

Vetting
Obtaining information of relevance to the security clearance assessment.

Appendix 2 – Meetings, visits and participation in conferences etc.

Brief descriptions of meetings, visits, seminars, conferences etc. in which the Committee and the Committee Secretariat have participated in 2015 are provided below. In addition to the listed events, the chair and other members of the Committee have also given talks about the EOS Committee's activities in some less formal contexts.

Visit to the Dutch oversight bodies
In January 2015, two committee secretariat employees visited the Dutch Review Committee on the Intelligence and Security Services (CTIVD) in the Hague as part of the efforts to increase the knowledge of other states' oversight of the secret services.

Democracy seminar in Bodø
In January 2015, the chair of the committee gave a talk about the oversight of the secret services in Norway at a democracy seminar on the terrorism threat, surveillance and security in a democratic society at the University of Nordland, Bodø.

Visit to the Swedish oversight bodies
In January 2015, two committee secretariat employees visited the Swedish Commission on Security and Integrity Protection in Stockholm as part of the efforts to increase the knowledge of other states' oversight of the secret services.

Meeting with the Parliamentary Ombudsman
In January, the Committee Secretariat met with members of the Parliamentary Ombudsman's staff. The purpose of the meeting was to exchange and learn from each other's experience.

Study trip to the USA
In January 2015, the senior social science adviser visited important American research environments in the field of surveillance and democratic oversight of secret services in Washington DC and Boston. The visit was part of the Committee's work to build a professional network and raise its competence in the field.

Visit by a delegation from Austria
In January 2015, the EOS Committee received a delegation from Austria. The visit was part of a study trip to Norway where the Austrian delegation wanted to learn more about the Norwegian oversight model for the secret services.

Visit by the Council of Europe Commissioner for Human Rights
In January 2015, the Council of Europe Commissioner for Human Rights, Mr Nils Muiznieks, visited the EOS Committee. The Commissioner wanted to learn more about the Norwegian oversight model for the secret services. Later in the year, the Commissioner published a report with recommendations – 'Democratic and effective oversight of national security service', the Council of Europe 2015.

Visit to DCAF
In January, the senior social science adviser visited the Geneva-based research institute Democratic Control of Armed Forces (DCAF). The object of the visit was to further develop contact and collaboration with the research centre.

Visit to the Belgian oversight bodies
In March 2015, the senior social science adviser visited the Belgian Standing Intelligence Agencies Review Committee in Brussels as part of the efforts to improve knowledge of other states' oversight of the secret services.

Meeting with the Ombudsman for the Armed Forces
In April 2015, committee secretariat employees met with the

Ombudsman for the Armed Forces to exchange experience and discuss common challenges, particularly as regards complaints in security clearance cases.

Researcher lunch in Tromsø

In May 2015, the head of the secretariat and two secretariat employees attended a researcher lunch with researchers and students from the Faculty of Law and the Faculty of Humanities, Social Sciences and Education at the University of Tromsø – the Arctic University of Norway. The topic for this meeting was the democratic oversight of the secret services in Norway and the EOS Committee's oversight function. The EOS Committee was co-organiser of the researcher lunch.

Participation at the OSCE conference in Uzbekistan

In May 2015, the senior social science adviser gave a talk at the Organization for Security and Co-operation in Europe's (OSCE) conference in Tashkent, Uzbekistan. The topic for the conference was 'Urgent issues of enhancement of organizational and legal mechanisms for exercise of Parliamentary control: National and foreign practice'.

European Parliament conference on democratic oversight of intelligence services

In May 2015, committee member Koritzinsky gave a lecture at the European Parliament's inter-parliamentary Conference on the Democratic oversight of Intelligence services in the European Union. The conference took place in Brussels.

Lecture at the Norwegian Defence Command and Staff College

In September 2015, committee member Koritzinsky and the senior social science adviser gave lectures about the EOS Committee to master's degree students on the school's intelligence course.

Data protection conference in Amsterdam

In October 2015, committee member Sunde and a secretariat employee attended the International Conference of Data Protection and Privacy Commissioners in Amsterdam.

Meeting with other states' oversight bodies in Bern

In October 2015, the head of the secretariat and the senior social science adviser met with representatives of several European countries' democratic oversight bodies for the secret services. At the meeting, the representatives discussed the possibility of increasing international collaboration between the oversight bodies.

Visit by a delegation from Germany

In October 2015, the Committee received a visit from the German G10 Commission of the German Bundestag. The visit was part of a study trip to Norway lasting for several days during which the German oversight commission wanted to learn more about the Norwegian oversight model for the secret services.

Book launch at the University of Oslo

In October 2015, the chair of the committee and the senior social science adviser gave talks at the international launch of the book Making International Intelligence Cooperation Accountable. The launch event took place at the Faculty of Law at the University of Oslo. The book is the result of a collaboration between the research centre DCAF, Durham University, UK, and the EOS Committee.

Half-day research seminar in Tromsø

In October 2015, the senior social science adviser gave a presentation on challenges relating to international collaboration between oversight bodies at a half-day seminar at the Faculty of Law at the University of Tromsø – the Arctic University of Norway. The EOS Committee was a co-organiser of the seminar.

Scandinavian meeting between oversight bodies in Stockholm

The EOS Committee and some of the secretariat employees met with their Scandinavian colleagues from Denmark and Sweden in October 2015. The topic of the meeting was challenges relating to the oversight of processing of personal data in the secret services. The meeting took place in Stockholm and lasted for two days.

Protection of privacy conference in Oslo

In October 2015, the head of the secretariat gave a lecture at the conference for data protection officers in Oslo. His topic was: 'Help – PST is at the door and wants our help. What do we do?'

DCAF Workshop – the Georgian parliament

In November, committee member Koritzinsky gave a lecture at the 'Intelligence and oversight reform in Georgia' workshop. The workshop was organised by the research centre DCAF.

Visit to American and Canadian oversight bodies

In November 2015, the senior social science adviser met with representatives of the U.S. Senate Select Committee on Intelligence and the U.S. House Permanent Select Committee on Intelligence, and the Canadian oversight bodies the Security Intelligence Review Committee and the Office of the Communications Security Establishment Commissioner. The visit was part of the efforts to improve knowledge of other states' oversight of the secret services.

Presentation to a parliamentary delegation from Ukraine

In November 2015, the senior social science adviser gave a presentation to a visiting Ukrainian parliamentary delegation. The topic of the presentation was how the EOS Committee keeps democratic oversight of the secret services in Norway.

Participation at DCAF conferences in the Western Balkans

In December 2015, the senior social science adviser gave the introductory speech at two conferences organised by DCAF in the Western Balkans (Macedonia and Slovenia).

The topic for both conferences was institutional development in young democracies, with particular focus on developing systems for democratic oversight of the secret services.

Appendix 3 – Act relating to Oversight of Intelligence, Surveillance and Security Service[49]

Section 1. The oversight agency and the oversight area

The Storting shall elect a committee for the oversight of intelligence, surveillance and security service carried out by, under the control of or on the authority of the public administration.

Such oversight shall not apply to any superior prosecuting authority.

The Public Administration Act and the Freedom of Information Act shall not apply to the activities of the Committee, with the exception of the Public Administration Act's provisions concerning disqualification.

The Storting shall issue an ordinary directive concerning the activities of the Oversight Committee within the framework of this Act and lay down provisions concerning its composition, period of office and secretariat.

The Committee exercises its mandate independently, outside the direct control of the Storting, but within the framework of laws and its directives. The Storting may, however, in regular joint decisions (Storting resolutions) order the committee to undertake specified investigations within the oversight mandate of the Committee, and under the auspices of the rules and framework which otherwise govern the Committee's activities.

Section 2. Purpose

The purpose of the oversight is:

1. to ascertain and prevent any exercise of injustice against any person, and to ensure that the means of intervention employed do not exceed those required under the circumstances, and that the services respect human rights,
2. to ensure that the activities do not involve undue damage to civic life,
3. to ensure that the activities are kept within the framework of statute law, administrative or military directives and non-statutory law.

The Committee shall show consideration for national security and relations with foreign powers.

The purpose is purely to oversee. The Committee may not instruct the bodies it oversees or be used by these for consultations.

Section 3. The responsibilities of the Oversight Committee

The Committee shall regularly oversee the practice of intelligence, surveillance and security services in public and military administration.

The Committee shall investigate all complaints from persons and organisations. The Committee shall on its own initiative deal with all matters and factors that it finds appropriate to its purpose, and particularly matters that have been subject to public criticism. Factors shall here be understood to include regulations, directives and established practice.

When this serves the clarification of matters or factors that the Committee investigates by virtue of its mandate, the Committee's investigations may exceed the framework defined in Section 1, first subsection, cf. Section 2.

Section 4. Right of inspection, etc.

In pursuing its duties, the Committee may demand access to the administration's archives and registers, premises, installations and constructions of all kinds. Establishments, etc. that are more than 50 per cent publicly owned shall be subject to the same right of inspection. The Committee's right of inspection and access pursuant to the first sentence shall apply correspondingly in relation to enterprises that assist in the performance of intelligence, surveillance, and security services.

All employees of the administration shall on request procure all materials, equipment, etc. that may have significance for effectuation of the inspection. Other persons shall have the same duty with regard to materials, equipment, etc. that they have received from public bodies.

Section 5. Statements, obligation to appear, etc.

All persons summoned to appear before the Committee are obliged to do so.

Persons making complaints and other private persons treated as parties to the case may at each stage of the proceedings be assisted by a lawyer or other representative to the extent that this may be done without classified information thereby becoming known to the representative. Employees and former employees of the administration shall have the same right in matters that may result in criticism of them.

All persons who are or have been in the employ of the administration are obliged to give evidence to the Committee concerning all matters experienced in the course of their duties.

An obligatory statement must not be used against any person or be produced in court without his consent in criminal proceedings against the person giving such statements.

The Committee may apply for a judicial recording of evidence pursuant to Section 43, second subsection, of the Courts of Justice Act. Sections 22-1 and 22-3 of the Civil Procedure Act shall not apply. Court hearings shall be held in camera and the proceedings shall be kept secret. The

49 Act No 7 of 3 February 1995 relating to the Oversight of Intelligence, Surveillance and Security Service (the Oversight Act)

proceedings shall be kept secret until the Committee or the competent ministry decides otherwise, cf. Sections 8 and 9.

Section 6. Ministers and ministries

The provisions laid down in Sections 4 and 5 do not apply to Ministers, ministries, or their civil servants and senior officials, except in connection with the clearance and authorisation of persons and enterprises for handling classified information.

Section 7.

(Repealed by the Act of 3 Dec. 1999 no. 82 (in force from 15 Oct. 2000 in acc. with Decree of 22 Sep. 2000 no. 958).)

Section 8. Statements and notifications

1. Statements to complainants shall be unclassified. Information concerning whether any person has been subjected to surveillance activities shall be regarded as classified unless otherwise decided. Statements to the administration shall be classified according to their contents.

   The Committee shall decide the extent to which its unclassified statements or unclassified parts of statements shall be made public. If it is assumed that making a statement public will result in revealing the identity of the complainant, the consent of this person shall first be obtained.
2. The Committee submits annual reports to the Storting about its activities. Such reports may also be submitted if factors are revealed that should be made known to the Storting immediately. Such reports and their annexes shall be unclassified.

Section 9. Duty of secrecy, etc.

With the exception of matters provided for in Section 8, the Committee and its secretariat are bound to observe a duty of secrecy unless otherwise decided.

The Committee's members and secretariat are bound by regulations concerning the handling of documents, etc. that must be protected for security reasons. They shall be authorised for the highest level of national security classification and according to treaties to which Norway is a signatory. The Presidium of the Storting is the security clearance authority for the Committee members. Background checks will be performed by the National Security Authority.

Should the Committee be in doubt as to the classification of information in statements or reports, or be of the opinion that certain information should be declassified or given a lower classification, the issue shall be put before the competent agency or ministry. The administration's decision is binding on the Committee.

Section 10. Assistance etc.

The Committee may engage assistance.

The provisions of the Act shall apply correspondingly to persons who assist the Committee. However, such persons shall only be authorised for a level of security classification appropriate to the assignment concerned.

Section 11. Penalties

Wilful or grossly negligent infringements of Section 4, first and third subsections of Section 5, first and second subsections of Section 9 and the second subsection of Section 10 of this Act shall render a person liable to fines or imprisonment for a term not exceeding one year, unless stricter penal provisions apply.

Section 12. Entry into force

This Act shall enter into force immediately.

Appendix 4 – Directive relating to Oversight of Intelligence, Surveillance and Security Service[50]

Section 1. On the Oversight Committee and its secretariat

The Committee shall have seven members including the chair and deputy chair, all elected by the Storting, on the recommendation of the Presidium of the Storting, for a period of no more than five years. Steps should be taken to avoid replacing more than four members at the same time.

The members of the Committee shall have the highest level of security clearance and authorisation, both nationally and according to treaties to which Norway is a signatory.

Remuneration to the Committee's members shall be determined by the Presidium of the Storting.

The chair of the Committee's secretariat shall be appointed and the chair's remuneration stipulated by the Presidium of the Storting on the basis of a recommendation from the Committee. Appointment and stipulation of the remuneration of the other secretariat members shall be made by the Committee. More detailed rules on the appointment procedure and the right to delegate the Committee's authority will be stipulated in personnel regulations to be approved by the Presidium of the Storting. The provision in the second subsection applies similarly to all employees in the secretariat.

Section 2. Quorum and working procedures

The Committee has a quorum when five members are present. The Committee shall as a rule function jointly, but may divide itself during inspection of service locations or installations.

In connection with particularly extensive investigations, the procurement of statements, inspections of premises, etc. may be carried out by the secretary and one or more members. The same applies in cases where such procurement by the full committee would require excessive work or expense. In connection with hearings, as mentioned in this Section, the Committee may engage assistance. It is then sufficient that the secretary or a single member participates.

The Committee may also otherwise engage assistance when special expertise is required.

Persons who have previously functioned in the intelligence, surveillance and security services may not be engaged to provide assistance.

Section 3. Procedure regulations

The secretariat keeps a case journal and minute book. Decisions and dissenting opinions shall appear from the minute book.

Statements and notes which appear or are entered in the minutes during oversight activities are not considered made unless communicated in writing.

Section 4. Oversight limitations etc.

The oversight activities do not include activities which concern persons or organisations not domiciled in Norway, or foreigners whose stay in Norway is in the service of a foreign state. The Committee can, however, exercise oversight in cases as mentioned above when special reasons so indicate.

The oversight activities should be exercised so that they pose the least possible disadvantage for the current activities of the services. The ministry appointed by the King can, in times of crisis and war, suspend the oversight activities in whole or in part until the Storting decides otherwise. The Storting shall be notified of such suspension immediately.

Section 5. Access limitations

The Committee shall not seek more extensive access to classified information than warranted by its oversight purposes. Insofar as possible, the concern for protection of sources and safeguarding of information received from abroad shall be observed.

Information received shall not be communicated to other authorised personnel or to other public bodies which are not already privy to them unless there is an official need for this, and it is necessary as a result of the oversight purposes or results from case processing provisions in Section 9. If in doubt, the provider of the information should be consulted.

Section 6. Disputes concerning access to information and oversight

The decisions of the Committee concerning what it shall seek access to and concerning the scope and extent of the oversight shall be binding on the administration. The responsible personnel at the service location concerned may demand that a reasoned protest against such decisions be recorded in the minutes. Protests following such decisions may be submitted by the head of the respective service and the Chief of Defence.

The protest shall, as mentioned here, be included in or enclosed with the Committee's annual report.

Section 7. On the oversight and statements in general

The Committee shall adhere to the principle relating to subsequent oversight. The Committee may, however, demand access to and make statements about current cases.

The Committee shall base its oversight and the formulation of its statements on the principles set down in Section 10, first subsection and Section 10, second subsection, first, third and fourth sentence, and Section 11 of the Act concerning the Storting's Ombudsman for public administration. The Committee may also propose improvements in administrative and organisational arrangements and routines where these can make oversight easier or safeguard against injustice being done.

Before making a statement in cases which may result in criticism or opinions directed at the administration, the head of the service in question shall be given the opportunity to make a statement on the issues raised by the case.

Statements to the administration shall be directed to the head of the service or body in question, or to the Chief of Defence or the competent ministry if the statement relates to matters they should be informed of as the commanding and supervisory authorities.

In connection with statements which contain requests to implement measures or make decisions, the recipient shall be asked to report on any measures taken.

Section 8. On complaints

On receipt of complaints, the Committee shall conduct such investigations of the administration as are appropriate in relation to the complaint. The Committee shall decide whether the complaint gives sufficient grounds for further action before making a statement.

Statements to complainants should be as complete as possible without revealing classified information. Statements in response to complaints against the Police Security Service concerning surveillance activities shall however only state whether or not the complaint contained valid grounds for criticism. If the Committee holds the view that a complainant should be given a more detailed explanation, it shall propose this to the Ministry concerned.

If a complaint contains valid grounds for criticism or other comments, a reasoned statement shall be addressed to the head of the service concerned or to the ministry concerned. Statements concerning complaints shall also otherwise always be sent to the head of the service against which the complaint is made.

Section 9. Procedures

Conversations with private individuals shall be in the form of an examination unless they are meant to merely brief the individual. Conversations with administration personnel shall be in the form of an examination when the Committee sees reason for doing so or the civil servant so requests. In cases

50 Directive relating to Oversight of Intelligence, Surveillance and Security service, adopted by a Storting resolution of 30 May 1995.

which may result in criticism being levied at individual civil servants, the examination form should generally be used.

The person who is being examined shall be informed of his or her rights and obligations, cf. Section 5 of the Act relating to the Oversight of Intelligence, Surveillance and Security Service. In connection with examinations that may result in criticism of the administration's personnel and former employees, said individuals may also receive the assistance of an elected union representative who has been authorised according to the Security Act with pertinent regulations. The statement shall be read aloud before being approved and signed.

Individuals who may become subject to criticism from the Committee should be notified if they are not already familiar with the case. They are entitled to familiarise themselves with the Committee's unclassified material and with any classified material they are authorised to access, insofar as this does not impede the investigations.

Anyone who submits a statement shall be presented with evidence and claims which do not correlate with their own evidence and claims, insofar as these are unclassified or the person has authorised access.

Section 10. Investigations at the ministries

The Committee cannot demand access to the ministries' internal documents.

Should the Committee desire information or statements from a ministry or its personnel in other cases than those which concern the ministry's handling of clearance and authorisation of persons and enterprises, these shall be obtained in writing from the ministry.

Section 11. Inspection

1. Responsibilities for inspection are as follows:
   a) For *the intelligence service*: to ensure that activities are carried out within the framework of the service's established responsibilities, and that no injustice is done to any person.
   b) For *the National Security Authority*: to ensure that activities are carried out within the framework of the service's established responsibilities, to oversee clearance matters in relation to persons and enterprises for which clearance has been denied, revoked, reduced or suspended by the clearance authorities, and also to ensure that no injustice is done to any person.
   c) For *the Police Security Service*: to oversee that the service's handling of preventive cases and investigations, its use of concealed coercive measures, its processing of personal data, and the exchange of information with domestic and foreign collaborative partners is carried out in accordance with current regulations, and meets the requirements for satisfactory routines within the framework of the purpose stated in Section 2 of the Act.
   d) For *the Defence Security Section*: to oversee that the service's exercise of personnel security clearance activities and other security clearance activities are kept within the framework of laws and regulations and the service's established responsibilities, and also to ensure that no injustice is done to any person.
   e) For *all services*: to ensure that the cooperation and exchange of information between the services is kept within the framework of service needs and applicable regulations.
2. Inspection activities shall, as a minimum, involve:
   a) half-yearly inspections of the Intelligence Service, involving accounts of current activities and such inspection as is found necessary.
   b) quarterly inspections of the National Security Authority, involving a review of matters mentioned under 1 b and such inspection as is found necessary.
   c) six inspections per year of the Central Unit of the Police Security Service, involving a review of new cases and the current use of concealed coercive measures, including at least ten random checks in archives and registers at each inspection, and involving a review of all current cases at least twice a year.
   d) three inspections per year of the Defence Security Service, including a review of the agency as a clearance authority, and a review of other security-related activities as found necessary.
   e) annual inspection of the PST entities in at least four police districts, at least two Intelligence Service units and/or intelligence/security services at military staffs and units and of the personnel security services of at least two ministries/government agencies.
   f) inspection of measures implemented on its own initiative by the remainder of the police force and by other bodies or institutions that assist the Police Security Service.
   g) other inspection activities indicated by the purpose of the Act.

Section 12. Information to the public

Within the framework of the third paragraph of Section 9 of the Act cf. Section 8, paragraph 1, the Committee shall decide what information shall be made public concerning matters on which the Committee has commented. When mentioning specific persons, consideration shall be given to protection of privacy, including persons not issuing complaints. Civil servants shall not be named or in any other way identified except by authority of the ministry concerned.

In addition, the chair or whoever the Committee authorises can inform the public of whether a case is being investigated and if the processing has been completed or when it will be completed.

Section 13. Relationship to the Storting

1. The provision in Section 12, first subsection, correspondingly applies to the Committee's notifications and annual reports to the Storting.
2. Should the Committee find that the consideration for the Storting's supervision of the administration dictates that the Storting should familiarise itself with classified information in a case or a matter the Committee has investi-

gated, the Committee must notify the Storting specifically or in the annual report. The same applies to any need for further investigation into matters which the Committee itself cannot pursue further.

3. By 1 April every year, the Committee shall report its activities in the preceding year to the Storting.
   The annual report should include:
   a) an overview of the composition of the Committee, its meeting activities and expenses.
   b) a statement concerning implemented supervision activities and the result of said activities.
   c) an overview of complaints by type and service branch, indicating what the complaints resulted in.
   d) a statement concerning cases and matters raised on the Committee's own initiative.
   e) a statement concerning any measures the Committee has requested be implemented and what these measures led to, cf. Section 6, fifth subsection.
   f) a statement concerning any protests pursuant to Section 5.
   g) a statement concerning any cases or matters which should be put before the Storting.
   h) the Committee's general experiences from the oversight activities and the regulations and any need for changes.

Section 14. Financial management, expense reimbursement for persons summoned before the Committee and experts

1. The Committee is responsible for the financial management of the Committee's activities, and stipulates its own financial management /directive. The directive shall be approved by the Presidium of the Storting.
2. Anyone summoned before the Committee is entitled to reimbursement of any travel expenses in accordance with the State travel allowance scale. Loss of income is reimbursed in accordance with the rules for witnesses in court.
3. Experts are remunerated in accordance with the courts' fee regulations. Higher fees can be agreed. Other persons assisting the Committee are reimbursed in accordance with the Committee scale unless otherwise agreed.

Appendix 5 – Statement from NIS – 'the Mathiesen mystery'

Statement on the EOS Committee's questions about Asbjørn Mathiesen

Introduction

NIS has searched its archives to find any documents of relevance to the case, and retired officers have been interviewed, two of whom had direct contact with Mathiesen in the course of their service. This information was then collated with the comprehensive information base for the Lund Commission's report. The service's statement about the case follows below.

The green network

The 'green network' was established shortly after World War II as a special telephone network primarily intended for use by government ministers. The first phones were green, hence the name. The reason why the network was established was a shortage of phone lines in post-war Oslo and the need for an overload-proof telephone network to guarantee that its users could communicate at any time even if the ordinary network were to break down. Such breakdowns could potentially be triggered by overloading of the ordinary telephone network or some other emergency that would put the ordinary system out of action. The task of installing and operating the network was assigned to the military intelligence service. The network was not intended to be secure against tapping. All the network users had a list of connected phone numbers on which it was stated that the network was only intended for unclassified calls. An increasing number of users were connected to the network, including the Chief of Defence and the head of the intelligence service. The 'green network' was wound up in 1987–88.

Asbjørn Mathiesen – technical consultant for the Intelligence Service

Engineer Asbjørn Mathiesen was originally employed by the engineering firm Henden, which was owned and run by engineer Audun Henden. Mathiesen later established his own business and took on assignments for the Intelligence Service as a consultant and on temporary contracts. Mathiesen was in charge of setting up the 'green network', and was responsible for its operation and maintenance during the period from 1945/46 to 1987. Documents from the service's archives show that Mathiesen was initially affiliated to the service's cipher office (office IV). Later, he received his assignments from the department in charge of technical information collection, which also had operational responsibility for the service's communication systems. The contract between Mathiesen and the Intelligence Service was terminated in 1987.

The Norwegian financial newspaper *Dagens Næringsliv* pointed out that Mathiesen was paid over the military intelligence service's secret budget. In connection with this, NIS would like to comment that, at this level of detail, the service's budgets have always been classified as secret.

Asbjørn Mathiesen's operational and maintenance responsibility for the 'green network'

Mathiesen was connected to the 'green network' via a phone installed in his home in Arnebråtenveien in the Hovseter area of Oslo. He could contact all other users connected to the network. Mathiesen was responsible for correcting errors in the network as required, a task that meant that he had to go to the network's exchange in the bunker at Ruseløkka. The Lund Commission's report (page 897) states that *'It is also*

clear that Asbjørn Mathiesen could access the green network from home to correct errors.' So, Mathiesen organised things so that he could correct network errors from his own home as a practical arrangement to avoid having to go down to the Ruseløkka bunker when he needed to do maintenance work on the network. This saved time for Mathiesen and was beneficial to the network's users, as it meant that the network would not be down for any length of time. Mathiesen had measuring equipment in his own home that he used to correct network errors. NIS has no information to indicate that he also had telephone surveillance equipment in his home. Former intelligence service officers who were in direct contact with Mathiesen emphasise that practical considerations were behind the arrangement whereby Mathiesen corrected errors from his own home.

Telephone cables to the head of the Intelligence Service and the Chief of Defence

According to *Dagens Næringsliv* and the Lund Commission's report, there was a phone line from the home of Egil Eikanger, the then head of the Intelligence Service, to Mathiesen's home about 300 metres away. When Eikanger became head of the Intelligence Service, he was connected to the 'green network', and a special phone line had to be installed from Eikanger's home to a network connection point, for example the Ruseløkka bunker. However, the closest connection point was in Mathiesen's home just 300 metres away, which is probably why Mathiesen chose this solution.

Similar practical considerations applied to the Chief of Defence. He was also connected to the green network, and a separate phone line had to be installed from his home to the nearest connection point. NIS knows that one Chief of Defence had his service residence in a side road to Ankerveien, which was closer to Mathiesen's home than to the Ruseløkka bunker.

NIS's investigation has not uncovered information confirming or disproving the existence of such cables. In any case, the crucial aspect is that it was possible for Mathiesen to correct network errors from home, and could in theory listen in on all calls on the network regardless of where the cables were, if he so wished and had phone tapping equipment available.

Possibilities for telephone surveillance

The following is stated on page 897 of the Lund Commission's report: *'It is also clear that Asbjørn Mathiesen could access the green network from home to correct errors.' According to the above-mentioned communications employee and the Commission's expert, this was arranged such that he could listen in on calls on the network from there. Asbjørn Mathiesen has denied this. He has nonetheless confirmed that only relatively simple and easily accessible additional equipment would be required for phone tapping to take place.'*

The following is quoted from page 904: *'It is also clear that, from a purely technical and practical perspective, it has been possible to listen in from the bunker on all calls made via the network. The same applies, with minor modifications, from Asbjørn Mathiesen's home.'*

In this connection, we would like to add that, at the time, the Intelligence Service had many switchboards where the operators and operations and maintenance personnel could tap the phones if they made an effort to. The fact that such networks could be tapped was as well known then as it is today. In this connection, reference is made to page 907 of the Lund Commission's report: *'Based on the description provided there, it is clear that it was technically possible to listen in on calls from the bunker. There is also information to indicate that Asbjørn Mathiesen could, at least with a little effort, listen in from his home. However, such tapping has not been the intention behind the technical solutions chosen and, with the possible exception of Asbjørn Mathiesen, it does not exceed what is technically possible at any telephone exchange or switchboard. The Commission has little information to suggest that telephone surveillance actually took place.'*

NIS would like to emphasise that the 'green network' for which Mathiesen had operational and maintenance responsibility was an unclassified network. During the period in question, the Intelligence Service had other communication systems in place to communicate highly classified information that could potentially be of interest to foreign powers. Mathiesen did not have access to these communication systems.

Dagens Næringsliv's story speculates about whether Mathiesen was tapping the 'green network' and providing information about calls to American or English parties. Former intelligence service officers who have been consulted as part of our investigation have stated that they cannot envisage Mathiesen engaging in any form of tapping of this unclassified network, nor understand what he would be listening for or which parties would be interested.

During its investigation, NIS has not uncovered information to indicate that Mathiesen took advantage of his position to tap the green network. Moreover, no information has emerged to indicate that intelligence service personnel instructed Mathiesen to do so.

Photo: IR Stone / Shutterstock.com

NORWEGIAN PARLIAMENTARY OVERSIGHT COMMITTEE
ON INTELLIGENCE AND SECURITY SERVICES

Contact information

Telephone: +47 23 31 09 30
Email: post@eos-utvalget.no
Postal address: PO box 84 Sentrum, N-0101 Oslo, Norway
Office address: Akersgata 8, Oslo

www.eos-utvalget.no