Renforcement de la surveillance des échanges de données internationaux entre les services de renseignement et de sécurité

Rédigée en coopération avec :

Belgian Standing Intelligence Agencies Review Committee
(Comité permanent de contrôle des services de renseignements et de sécurité / Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten)
www.comiteri.be

Danish Intelligence Oversight Board
(Tilsynet med Efterretningstjenesterne)
www.tet.dk

Review Committee on the Intelligence and Security Services – The Netherlands
(Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten)
www.ctivd.nl

EOS Committee – The Norwegian Parliamentary Intelligence Oversight Committee
(EOS-utvalget)
www.eos-utvalget.no

Independent Oversight Authority for Intelligence Activities (OA-IA)
(Autorité de surveillance indépendante des activités de renseignement AS-Rens)
www.ab-nd.admin.ch

Belgian Standing Intelligence Agencies Review Committee

tet
Danish Intelligence Oversight Board

CT IVD

EOS COMMITTEE
NORWEGIAN PARLIAMENTARY OVERSIGHT COMMITTEE
ON INTELLIGENCE AND SECURITY SERVICES

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

1. Objet

Cinq organes de surveillance européens ont entamé une nouvelle forme de coopération.

La présente déclaration a pour but de :

- Décrire notre projet, qui consistait pour chacun d'entre nous à examiner l'usage fait par nos propres services des informations relatives aux combattants terroristes étrangers ainsi qu'à mettre en commun nos méthodes, meilleures pratiques et expériences ;

- Relever les défis rencontrés dans le cadre de la surveillance des échanges de données internationaux, y compris le risque de lacunes dans la surveillance inhérent à la coopération internationale entre les services de renseignement et de sécurité ;

- Identifier des moyens de renforcer la coopération en matière de surveillance, par exemple en réduisant l'obligation du secret entre les organes de surveillance pour pouvoir partager certaines informations et améliorer ainsi notre surveillance des échanges internationaux.

2. Introduction

Les attaques terroristes récentes, comme celles de Paris, Bruxelles et Londres, ont été exécutées par des personnes commanditées, encouragées ou inspirées par l'EI, Al-Qaïda ou d'autres groupes terroristes. L'identification et l'analyse de la menace posée par des combattants terroristes formés dans leur pays de résidence et par le retour de combattants terroristes étrangers sont des tâches importantes des services de renseignement et de sécurité dans toute l'Europe.

La menace du terrorisme djihadiste n'a cessé de se complexifier et de s'étendre ces dernières années. Une coopération internationale — bilatérale ou multilatérale — entre les services de renseignement et de sécurité est nécessaire pour enquêter sur cette menace. Une telle coopération existe en Europe et avec d'autres pays. L'intensification de cette coopération a eu pour corollaire une augmentation des échanges de données personnelles entre les services. Les échanges de données avec des services étrangers font partie des tâches quotidiennes des services de renseignement et de sécurité. Les données peuvent être échangées de différentes manières, oralement ou par écrit.

Les organes de surveillance ont naturellement suivi le développement de la coopération internationale entre les services de renseignement et de sécurité. Notre mandat étant strictement national, nous avons été préoccupés par le risque qu'une lacune se produise dans la surveillance. Dans l'idéal, les systèmes nationaux de surveillance seraient complémentaires : là où un organe de surveillance atteindrait les limites de son mandat national, un autre aurait la compétence d'assurer efficacement la surveillance. Toutefois, il peut arriver que la législation nationale sur les échanges de données et leur surveillance ne réponde pas à ces critères. En outre, la coopération internationale entre les services de renseignement pourrait évoluer de manière à ce que la surveillance nationale ne puisse plus la suivre, ce qui entraînerait un déficit de responsabilité ou une lacune dans la surveillance.

En conséquence, les cinq organes de surveillance de la Belgique, du Danemark, des Pays-Bas, de la Norvège et de la Suisse ont décidé de monter un projet commun pour échanger leurs expériences et méthodes. Chaque organe a mené sa propre enquête nationale, portant sur les échanges de données internationaux concernant les combattants terroristes étrangers, auprès des services de renseignement et de sécurité placés sous sa supervision.[1]

Nous avons mené nos investigations plus ou moins en même temps, chacun pour son État et dans le cadre de son mandat national. Nous nous sommes réunis régulièrement pour comparer nos méthodes d'investigation, interpréter les cadres légaux, discuter de problèmes juridiques et pratiques et rassembler nos résultats et conclusions. Nous n'avons pas échangé d'informations classifiées.

[1] The Report from CTIVD (The Netherlands) about the investigation in Englisch – https://english.ctivd.nl/latest/news/2018/04/26/index
Annual Report Danish Intelligence Oversight Board in Englisch – http://www.tet.dk/redegorelser/?lang=en

3. Pratiques actuelles en matière de surveillance des échanges de données

Les organes de surveillance qui participent au projet supervisent les échanges de données entre les services de renseignement et de sécurité de diverses façons. Ils peuvent

- Évaluer des relations ou arrangements de coopération entre des services de renseignement et de sécurité ;
- Évaluer la légitimité et la qualité des échanges de données spécifiques avec des services étrangers;
- Examiner le système d'échange de données dans son ensemble, y compris les garanties ;
- Participer à des procédures concernant des réclamations et des recours individuels.

Bien que les mandats des organes de surveillance diffèrent, tous disposent d'un large éventail d'instruments pour surveiller les échanges de données internationaux.

Évaluation des rapports de coopération

Les organes de surveillance peuvent évaluer si les rapports de coopération entre leur service national et les services partenaires d'autres pays respectent certains critères. La loi régissant les services de renseignement et de sécurité peut définir des critères de coopération. Ceux-ci tiennent généralement compte de la nécessité de la coopération, du respect des droits de l'homme et de l'existence d'une législation sur la protection et/ou la fiabilité des données. Le seuil de la coopération avec des services qui ne remplissent pas les critères devrait être élevé. Les organes de surveillance de la Belgique, des Pays-Bas, de la Norvège et de la Suisse examinent les considérations formulées par leurs services nationaux.

Les rapports de coopération entre les services peuvent être basés sur des accords, tels que des déclarations d'intention ou des protocoles d'entente. S'ils ne sont généralement pas juridiquement contraignants, ces accords offrent un cadre pratique pour les échanges de données entre services. L'existence même de certains de ces accords constitue une information classifiée, alors que d'autres accords sont publiés par des gouvernements ou des services. Néanmoins, ils peuvent établir un cadre pour les rapports de coopération en réglant des questions telles que le but de la coopération, ses modalités, ses restrictions en matière de divulgation à des tiers ou ses aspects procéduraux. Les organes de surveillance des cinq pays peuvent procéder à un examen ou faire un rapport sur la conformité de ces accords avec les lois et réglementations nationales.

Évaluation de la légitimité des échanges de données spécifiques

Les organes de surveillance peuvent évaluer si des échanges de données individuels satisfont aux exigences légales imposées par les lois et réglementations nationales.

Nos lois nationales présentent certaines caractéristiques communes, notamment les principes de nécessité et de proportionnalité, lesquels découlent de cadres juridiques internationaux tels que la Convention

européenne des droits de l'homme. Le principe de nécessité implique l'existence d'un but clair et légal pour l'échange de données ainsi que celle de motifs raisonnables permettant de croire que ce but sera atteint en échangeant les données. Le principe de proportionnalité oblige le service à trouver un juste équilibre entre le but de l'échange et la gravité d'une éventuelle atteinte aux droits fondamentaux. La plupart des lois nationales contiennent encore d'autres exigences, comme le caractère raisonnable, la rectitude, l'efficacité et la fiabilité de l'échange de données.

La gestion interne des services peut prévoir des règles supplémentaires pour les échanges de données. Elle peut par exemple préciser le type d'échange de données autorisé et les circonstances entourant l'échange, le niveau d'autorisation exigé et l'utilisation potentielle des données reçues. En l'absence d'une loi nationale ou d'accords bilatéraux ou multilatéraux, ou de toute précision sur des questions particulières, la gestion interne peut offrir des garanties supplémentaires.

Évaluation de la qualité des échanges de données spécifiques

La qualité peut se rapporter au contenu ou au format des données. En ce qui concerne le contenu, la qualité signifie que les données sont correctes, formulées de manière suffisamment claire et précise, confirmées par des données sous-jacentes, actualisées et dotées d'une indication de probabilité ou de fiabilité. Quant au format, les aspects qualitatifs se rapportent à la mention d'un niveau de classification, de la date de l'échange, du nom du (des) service(s) partenaire(s) destinataire(s) et des réserves concernant l'utilisation des données. Chacun des cinq organes de surveillance peut vérifier la qualité de l'échange de données à cet égard.

La qualité peut aussi avoir une signification différente : elle peut se rapporter à l'efficience ou à l'efficacité de l'échange de données, c'est-à-dire à sa pertinence, son opportunité temporelle et l'atteinte de son objectif. Ce type d'examen de la qualité est moins fréquent chez les organes de surveillance. Les organes de surveillance de la Belgique et de la Suisse sont expressément autorisés à vérifier si un échange de données a été efficace et efficient.

Examen du système d'échange de données dans son ensemble

Les organes de surveillance peuvent adopter une approche plus large lors de l'examen de la légitimité des échanges de données. En examinant certains cadres de coopération multilatérale, l'organe de surveillance des Pays-Bas considère expressément le système d'échange de données dans son ensemble et s'intéresse à la protection des droits individuels à l'intérieur de ce système. Même si certains échanges de données spécifiques sont légitimes, les garanties systémiques peuvent s'avérer insuffisantes pour assurer leur légitimité à long terme. Ce type de vérification peut contribuer à prévenir des échanges de données illégaux entre des services de renseignement et de sécurité.

Une approche similaire peut être adoptée lors de l'examen de la qualité de l'échange de données. Si le but de l'échange de données est de contrer le terrorisme djihadiste, sa qualité globale pourrait être mesurée en vérifiant la quantité des informations partagées ayant conduit à la poursuite et à la condamnation, ou même directement à la prévention d'une attaque terroriste. Toutefois, cette manière de mesurer l'utilité des données échangées peut s'avérer problématique, car ces investigations ont souvent lieu après coup. L'organe de surveillance détermine alors si les données pertinentes ont été suffisamment et adéquatement échangées avec les partenaires nationaux et internationaux. L'organe de surveillance belge a été impliqué dans ce type d'examen.

Implication dans les réclamations et recours individuels

En général, les organes de surveillance de chacun des cinq pays peuvent recevoir des réclamations individuelles concernant les activités des services de renseignement et de sécurité. Ils peuvent habituellement donner des avis ou des recommandations qui ne sont pas juridiquement contraignants aux services de renseignement et de sécurité et aux ministres politiquement responsables. En règle générale, les services se conforment à ces avis et recommandations. Une nouvelle loi adoptée en 2017 aux Pays-Bas autorise l'organe de surveillance à prendre des décisions contraignantes concernant les réclamations. Ceci peut également inclure l'ordre de mettre fin à l'exercice d'une compétence ainsi que la destruction ou le retrait de données traitées.

Le secret nécessaire au déroulement des activités des services de renseignement et de sécurité limite généralement le droit des particuliers à accéder à leurs données personnelles. Certains pays autorisent explicitement les particuliers à demander à l'organe de surveillance national d'examiner les données personnelles qui ont été traitées par leurs services et qui les concernent. Au Danemark, toute personne peut demander à l'organe de surveillance danois de vérifier si le service de sécurité traite illégalement des données personnelles la concernant. Dans le cas du service de renseignement militaire, cet examen est limité aux résidents. Dans les deux cas, l'organe de surveillance danois peut exiger la suppression des données personnelles concernant l'auteur de la demande.

En Belgique, l'organe de surveillance doit examiner toutes les réclamations qui ne sont pas manifestement infondées. L'intéressé recevra les conclusions de l'enquête en termes généraux. Il pourra ensuite utiliser celles-ci en justice ou devant une autorité administrative. Dans certains cas, l'organe de surveillance doit donner un avis officiel à une cour pénale après une réclamation. Il peut prendre des décisions contraignantes suite aux réclamations portant sur deux autres objets (utilisation de méthodes spéciales et protection des données).

En Norvège, les résidents ont aussi le droit d'adresser des réclamations à l'organe de surveillance en cas de soupçon de surveillance illégale. Toutefois, l'organe de surveillance norvégien n'a pas le pouvoir d'ordonner la suppression des données. En Suisse, le préposé fédéral à la protection des données et de l'information (PFPDI) est chargé de traiter les demandes concernant le traitement des données.

4. Défis de la surveillance des échanges de données internationaux

Dans le cadre de notre projet, nous avons constaté que le renforcement de la coopération et des échanges de données, notamment au niveau multilatéral, entre les services de renseignement et de sécurité, peuvent poser des défis juridiques et pratiques aux organes de surveillance.

La surveillance s'arrête aux frontières nationales

La législation nationale promeut souvent la coopération et l'échange d'informations entre les services de renseignement et de sécurité, aussi bien au niveau bilatéral que multilatéral. Toutefois, elle ne fournit généralement pas les bases légales spécifiques permettant aux organes de surveillance de coopérer ou d'échanger des informations concernant des particuliers. Aucun des cinq organes représentés dans la présente déclaration ne dispose de bases légales expresses lui permettant d'échanger des données avec un autre organe de surveillance, et certainement pas lorsqu'il s'agit d'informations classifiées.

Si les services de renseignement et de sécurité traversent les frontières nationales, les organes de surveillance ne le peuvent pas, car leur compétence se limite à des mandats nationaux. La surveillance ne reflète qu'un aspect de l'échange de données, car elle se concentre soit sur la fourniture de données et leur collecte préalable, soit sur la réception de données et leur utilisation. Les organes de surveillance nationaux ne peuvent pas obtenir de manière indépendante une image complète des échanges de données personnelles, et encore moins vérifier la légalité de l'ensemble du processus d'échange de données.

La limitation des activités à la surveillance nationale ne constitue pas nécessairement une lacune en matière de contrôle. L'existence d'une surveillance exhaustive et efficace des deux côtés de la frontière prévient la formation de lacunes entre les mandats des organes de surveillance. Néanmoins, quand il s'agit d'une coopération — principalement multilatérale — entre des services de renseignement et de sécurité, la coopération des organes de surveillance est seulement aussi solide que son maillon le plus faible.

Le défi de la coopération face au secret

La compétence des organes de surveillance est limitée par les règles nationales en matière de secret. Ils ne peuvent diffuser et évoquer que des informations désignées publiques extraites de leurs recherches. En pratique, cela signifie qu'ils n'ont qu'un très faible aperçu de ce qui se passe de « l'autre côté » de l'échange de données, à savoir si une surveillance est effectivement exercée ou s'il existe une lacune dans le contrôle. En conséquence, les organes de surveillance sont non seulement dans l'impossibilité de travailler hors des frontières, mais encore dans l'incapacité notable d'aborder avec d'autres organes de surveillance les événements se déroulant à l'intérieur de leurs propres frontières.

À mesure que notre projet commun avançait, nous avons remarqué à plusieurs occasions que nous ne pouvions même pas discuter de questions connues de nous tous, comme le contenu d'accords conclus

entre les services que nous surveillons. En outre, nous avons constaté qu'une information peut être publique dans un pays et confidentielle dans un autre. Cette situation a compliqué la tâche des membres du projet en limitant la possibilité de mener une discussion de fond sur les sujets en question.

Évaluation de la nécessité et de la proportionnalité

Comme indiqué précédemment, les organes de surveillance évaluent en permanence la nécessité et la proportionnalité d'un échange de données par rapport à une finalité précise. Ils doivent donc tenir compte du niveau de la protection des droits individuels accordée par le service destinataire. Cela devient de plus en plus difficile à mesure que le volume des échanges de données et le nombre de services étrangers avec lesquels les données sont partagées augmentent. Le critère de nécessité et de proportionnalité peut devenir abstrait et perdre de sa substance lorsque les données échangées sont moins précises ou échangées à l'intérieur d'un plus grand groupe de services de renseignement et de sécurité.

Les normes concernant la légitimité et la qualité applicables à la collecte, au traitement, à la conservation et à l'échange de données peuvent varier d'un État à l'autre. Le niveau de la protection des droits individuels accordée par le service destinataire des données est important dans l'évaluation de la proportionnalité d'un échange de données en particulier. Il n'est pas toujours facile à déterminer, car les services de renseignement et de sécurité ne sont pas nécessairement ouverts à propos de tous les aspects du cadre juridique en place et des normes qu'ils appliquent.

Dans le cadre des échanges de données multilatéraux, des normes et définitions communes pourraient contribuer à définir les conditions dans lesquelles l'échange de données est jugé nécessaire et proportionné ainsi que le niveau minimal de la protection des données requise pour préserver efficacement les droits individuels. Il est de l'intérêt de toutes les parties — services de renseignement et de sécurité et organes de surveillance — d'adopter des normes communes et de s'accorder sur l'interprétation des garanties légales existantes. Cela peut également contribuer à la légitimité de l'échange multilatéral en question.

Certains pays font la distinction entre citoyens et étrangers

Certains cadres juridiques nationaux offrent un niveau de protection plus élevé à leurs ressortissants ou résidents qu'aux étrangers ou aux non-résidents. Le cas échéant, les ressortissants et résidents ont également un accès privilégié aux recours individuels. Cette distinction peut limiter ou exclure l'accès aux recours individuels pour les étrangers et non-résidents dont les données ont été échangées par le service de renseignement ou de sécurité respectif.

Une distinction similaire peut affecter le mandat d'un organe de surveillance dont la compétence est parfois limitée au seul examen des échanges de données concernant des nationaux ou des résidents. L'obtention de données relatives à d'autres personnes n'est alors pas de son ressort. Si aucun autre organe de surveillance ne peut examiner efficacement cette partie de l'échange de données, il existe une lacune en matière de contrôle.

Moyens et méthodes pour les échanges de données

Les services de renseignement et de sécurité s'échangent les données de différentes manières, dont certaines créent des défis supplémentaires pour les organes de surveillance. C'est le cas par exemple lors des échanges de données informels. Comment surveiller efficacement des données échangées pendant des conférences et des réunions, ou par téléphone, etc. ? L'augmentation des échanges de données internationaux peut obliger les organes de surveillance à trouver de nouvelles méthodes de surveillance, car il n'est plus possible de contrôler chaque échange de données individuellement. En ce qui concerne la protection des données, les développements observés dans les échanges de données multilatéraux peuvent engager des responsabilités du côté des services participants comme de celui des organes de surveillance. Pour préserver efficacement les droits individuels, les services de renseignement et de sécurité pourraient être contraints à publier les normes qu'ils appliquent et à fixer un niveau minimal de la protection [des droits individuels] accordée par tous les services participants.

5. Surveillance des échanges de données internationaux — des progrès

Notre projet nous a montré que les efforts consentis par les services de renseignement et de sécurité pour échanger plus efficacement les données, notamment au niveau multilatéral, ainsi que la forte augmentation du volume des données échangées, ont suscité de nouveaux défis pour les organes de surveillance. Il s'agit tant des limitations inhérentes aux mandats nationaux des organes de surveillance et de l'incapacité de ces derniers à évoquer entre eux des échanges de données internationaux que de leurs propres efforts consentis pour apporter des innovations aux procédures et méthodes visant à garantir une surveillance efficace.

La souveraineté et les intérêts nationaux dictent la marche à suivre en matière de coopération internationale entre les services de renseignement et de sécurité. Il est logique que, contrairement à d'autres domaines de la coopération internationale, la surveillance des services de renseignement et de sécurité continue d'être assurée par des organes nationaux. Toutefois, si les services de renseignement et de sécurité ignorent les frontières nationales, les organes de surveillance restent quant à eux cantonnés au territoire national. Par conséquent, la surveillance reflète toujours un seul côté de l'échange de données. De plus, les organes de surveillance sont largement incapables d'aborder avec d'autres organes de surveillance les résultats obtenus à la suite de l'examen d'un échange de données. En raison de ces limitations inhérentes à la surveillance nationale, il existe un risque de lacune dans le contrôle des échanges de données internationaux entre services de renseignement et de sécurité. La question est de savoir comment juguler ce risque.

En partageant leurs connaissances, expériences et méthodes d'investigation et en comparant leurs résultats, conclusions et recommandations, les organes de surveillance peuvent se rapprocher. Notre expérience a montré que c'est précisément le résultat que notre projet commun a permis d'atteindre. Nous avons tiré profit des meilleures pratiques des uns et des autres, développé une meilleure compréhension des systèmes juridiques de chacun d'entre nous et établi des rapports de confiance. Intensifier notre coopération est exactement ce que nous devons faire pour permettre aux organes de surveillance de rester dans la course au vu de l'évolution de la coopération internationale entre les services de renseignements et de sécurité.

Une mesure importante et constructive vers une coopération plus étroite consiste à diminuer les impératifs de confidentialité lors des échanges d'informations entre organes de surveillance. Ces derniers pourraient au minimum parler des accords de coopération bilatéraux et multilatéraux passés entre les services de renseignement et de sécurité qu'ils surveillent. Une autre mesure logique serait de partager avec d'autres organes de surveillance des informations qui ont déjà été échangées par les services de renseignement et de sécurité eux-mêmes. Une fois que des données ont été échangées, il n'y a aucune raison pour que le contrôle reste à la traîne. Nous ne disons pas pour autant qu'il faut éliminer toutes les restrictions imposées par les normes nationales régissant la confidentialité des informations. Au contraire, la coopération entre les organes de surveillance devrait se dérouler dans les limites et conformément aux normes arrêtées par les législateurs nationaux.

Le fait de pouvoir s'entretenir d'accords de coopération et des échanges de données internationaux avec d'autres organes de surveillance comporte aussi certaines responsabilités. Protéger adéquatement les

droits individuels tout en coopérant au niveau international implique une certaine transparence des services de renseignement et de sécurité par rapport aux normes qu'ils appliquent, mais aussi une contribution avérée à l'établissement d'un niveau de protection minimal identique de la part de tous les services participants. Les organes de surveillance doivent aussi respecter ce niveau de protection minimal des données et rechercher un terrain d'entente sur l'interprétation des garanties légales existantes.

Compte tenu de l'évolution technologique et du renforcement de la coopération, les échanges de données entre les services de renseignement et de sécurité s'intensifient et entraînent aussi une hausse du nombre des échanges individuels de données. Le volume même des données échangées risque de devenir un enjeu majeur. L'évaluation de la légitimité et de la qualité de chaque échange individuel peut être une charge colossale pour les organes de surveillance. S'ajoutant aux vérifications ponctuelles, l'évaluation du système et du cadre de l'échange de données ainsi que de l'existence et de l'efficacité de garanties pour assurer la protection des droits fondamentaux s'avère de plus en plus importante.

Pour atteindre efficacement cet objectif, les organes de surveillance devront mettre au point de nouvelles méthodes. L'automatisation permise par les ordinateurs et les outils élaborés pour surveiller de grandes quantités de données se profilent en tant que solutions possibles. Dans cette optique, les organes de surveillance doivent élargir leur expertise informatique et leurs connaissances des systèmes utilisés par les différents services. Une prise en compte des besoins des organes de surveillance lors de la mise en œuvre de nouveaux systèmes par les services ainsi que le renforcement des mécanismes de contrôle interne et externe contribueraient également à garantir un contrôle efficace.

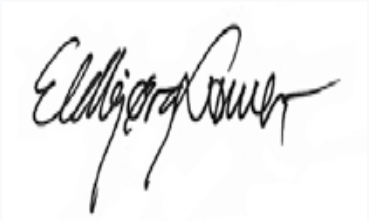
Les organes de surveillance de la Belgique, du Danemark, des Pays-Bas, de la Norvège et de la Suisse continueront d'échanger leurs méthodes et meilleures pratiques et de discuter des défis internationaux relatifs à la surveillance ainsi que des meilleures approches permettant de les surmonter. Nous invitons les organes de surveillance d'autres pays à nous rejoindre dans nos efforts pour limiter le risque d'une lacune de contrôle et améliorer la surveillance des échanges internationaux de données entre les services de renseignement et de sécurité.

Signée à Berne le 22 octobre 2018,

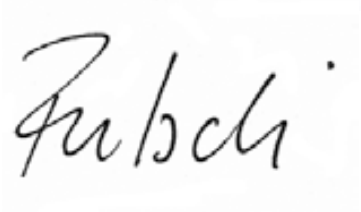
Mr. Serge Lipszyc, Vorsitzender Belgian Standing Intelligence Agencies Review Committee

Mr. Michael Kistrup, Vorsitzender Danish Intelligence Oversight Board

Mr. Harm Brouwer, Vorsitzender Dutch Review Committee on the Intelligence and Security Services



Mrs. Eldbjørg Løwer, Vorsitzende EOS Committee – The Norwegian Parliamentary Intelligence Oversight Commit-tee



Mr. Thomas Fritschi, directeur de l'Autorité de surveillance indépendante des activités de renseignement AS-Rens

De gauche à droite: Harm Brouwer (chair CTIVD, the Netherlands), Thomas Fritschi (Leiter AB-ND, Schweiz), Eldbjorg Lower (chair EOS Committee, Norway), Serge Lypszyc (chair Comité I, Belgium). Michael Kistrup, Chair of the Danish oversight board, n'est pas sur la photo