Renforcement du contrôle des échanges internationaux de données entre les services de renseignement et de sécurité

Co-rédigé par:

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)
(Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND)
www.ab-nd.admin.ch

Belgian Standing Intelligence Agencies Review Committee

tet
Danish Intelligence Oversight Board

CTIVD
Review Committee on the Intelligence and Security Services

EOS COMMITTEE
NORWEGIAN PARLIAMENTARY OVERSIGHT COMMITTEE ON INTELLIGENCE AND SECURITY SERVICES

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

1. Contenu

Cinq organes de contrôle européens des services de renseignement ont initié une nouvelle forme de coopération. Dans la présente déclaration, nous :

- Décrirons notre projet, qui a amené chacun de nous à réaliser une enquête sur l'utilisation, par nos services nationaux respectifs, des informations concernant les *foreign terrorist fighters* et à partager ses méthodes, ses meilleures pratiques et ses expériences.

- Aborderons les défis auxquels nous sommes confrontés dans le cadre du contrôle effectué sur les échanges internationaux de données, y compris le risque de lacunes en matière de contrôle dans le contexte de la coopération entre les services de renseignement au niveau international.

- Identifierons des voies de progrès pour un renforcement de la coopération en matière de contrôle, par exemple en limitant le secret entre les organes de contrôle, et ce afin de permettre l'échange de certaines informations. L'objectif étant d'améliorer notre contrôle sur les échanges internationaux de données.

2. Introduction

Les récents attentats terroristes, comme ceux qui ont touché Paris, Bruxelles et Londres, ont été perpétrés par des personnes téléguidées, encouragées ou inspirées par l'EIIL, Al-Qaeda ou des groupes terroristes similaires. Identifier et analyser la menace que constituent les returnees et les *homegrown terrorist fighters* est une mission importante des services de renseignement et de sécurité dans toute l'Europe.

Au cours de ces dernières années, la menace du terrorisme djihadiste s'est répandue et a gagné en complexité. Analyser cette menace requiert une coopération internationale entre les services de renseignement et de sécurité, tant au niveau bilatéral que multilatéral. Une telle coopération existe en Europe et avec d'autres pays. L'intensification de cette coopération va de pair avec l'accroissement des échanges de données à caractère personnel. Échanger des données avec des services étrangers fait partie des activités quotidiennes des services de renseignement et de sécurité. Les données peuvent être échangées de différentes manières, que ce soit oralement ou par écrit.

Les organes de contrôle ont naturellement suivi le développement de la coopération internationale entre les services de renseignement et de sécurité. Nos mandats de contrôle respectifs étant strictement nationaux, nous nous sommes intéressés au risque de lacunes dans le contrôle. Idéalement, les systèmes nationaux de contrôle devraient être complémentaires. Ainsi, lorsqu'un organe de contrôle atteint les limites de son mandat national, l'autre est compétent pour exercer un contrôle efficace. Cependant, la législation nationale en matière d'échanges d'informations et le contrôle de ces échanges peuvent ne pas satisfaire à ces exigences. En outre, la coopération internationale entre les services de renseignement pourrait se développer de telle manière que le contrôle national ne pourrait plus être exercé comme il se doit. Il pourrait alors en résulter un « déficit de responsabilité » ou une « lacune dans le contrôle ».

À la lumière de ce qui précède, les cinq organes de contrôle belge, danois, néerlandais, norvégien et suisse ont décidé de lancer un projet visant à échanger leurs expériences et leurs méthodes. Chacun de ces organes de contrôle a mené une enquête au niveau national sur les échanges internationaux de données relatifs aux *foreign terrorist fighters* entre les services de renseignement et de sécurité soumis à leur contrôle.[1]

Nous avons mené nos enquêtes respectives plus au moins au même moment, à partir de notre contexte national et dans le cadre de notre mandat national. Nous nous sommes régulièrement réunis pour comparer nos méthodes d'enquête, interpréter les cadres juridiques, discuter des problèmes juridiques et pratiques et collationner nos constatations et nos conclusions. Aucune information classifiée n'a été échangée.

[1] Rapport du CTIVD (Pays-Bas) concernant l'enquête, en anglais - https://english.ctivd.nl/latest/news/2018/04/26/index
Rapports annuels, en anglais, de l'Organe de contrôle des services de renseignement danois (Danish Intelligence Oversight Board) - http://www.tet.dk/ redegorelser/?lang=en

3. Pratiques en vigueur en matière de contrôle des échanges de données

Les organes de contrôle participants contrôlent les échanges de données entre les services de renseignement et de sécurité de différentes manières. Nous pouvons :

- Évaluer les relations ou les mécanismes entre les services de renseignement et de sécurité ;
- Évaluer la légitimité et la qualité d'échanges de données spécifiques avec des services étrangers ;
- Revoir le système d'échange de données dans son ensemble, y compris les garde-fous ;
- Être impliqués dans des procédures relatives aux recours et plaintes individuels.

Les mandats des organes de contrôle sont certes différents, mais nous disposons tous d'une large gamme d'instruments nous permettant de contrôler les échanges internationaux de données.

Évaluation du lien de coopération

Les organes de contrôle peuvent évaluer si le lien de coopération entre leur service national et les services partenaires d'autres pays répond à certains critères. La législation organique des services de renseignement et de sécurité peut définir des critères spécifiques de coopération. Généralement, les critères incluent la nécessité de coopérer, le respect des droits de la personne, l'existence d'une législation sur la protection des données et/ou la fiabilité. Il conviendrait de placer la barre très haut pour ce qui relève de la coopération avec des services qui ne respectent pas les critères. Les organes de contrôle belge, néerlandais, norvégien et suisse évaluent les considérations émises à cet égard par leurs services nationaux.

Les liens de coopération entre les services peuvent s'appuyer sur des accords, par exemple des lettres d'intention ou memorandums of understanding. De tels accords ne sont généralement pas contraignants sur le plan juridique mais offrent un cadre pratique pour les échanges de données par les services. L'existence de certains de ces accords est même classifiée. D'autres accords sont rendus publics par les gouvernements ou les services. Ils peuvent néanmoins tracer les contours des liens de coopération en abordant la question de l'objectif visé par la coopération, les attentes en termes de fonctionnement de la coopération, les restrictions liées à la divulgation à des tiers ou les aspects procéduraux de la coopération. Les organes de contrôle des cinq pays peuvent contrôler si ces accords respectent les lois et les réglementations nationales ou faire rapport à ce sujet.

Évaluation de la légitimité d'échanges de données spécifiques

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

Les législations nationales de nos pays partagent certaines caractéristiques, plus particulièrement les principes de nécessité et de proportionnalité. Ces principes partagés trouvent leur source dans les cadres légaux internationaux tels que la Convention européenne des droits de l'homme. Le principe de nécessité inclut le critère d'une finalité légale claire pour l'échange de données et une attente raisonnable en termes de résultat à atteindre via l'échange de données. En vertu

du principe de proportionnalité, le service se doit de concilier la finalité de l'échange et la gravité de la violation des droits fondamentaux. La plupart des législations nationales renferment encore d'autres exigences, comme le caractère raisonnable, la justesse, l'efficacité et la fiabilité de l'échange d'informations.

La politique interne des services peut définir des règles additionnelles en matière d'échanges de données. Une telle politique peut, par exemple, spécifier quel type d'échange de données est autorisé, dans quelles circonstances, quel niveau d'autorisation est requis et quel usage peut être fait des données obtenues. En l'absence de loi nationale ou d'accords bilatéraux et multilatéraux, ou si ceux-ci passent sous silence un point précis, la politique interne peut offrir des garanties supplémentaires.

Évaluation de la qualité d'échanges de données spécifiques

La qualité peut se rapporter au contenu des données ou du format des données. S'agissant du contenu, la qualité signifie que les données sont correctes, suffisamment claires et précises dans leur libellé, confirmées par des données sous-jacentes, actualisées, et qu'elles comportent une indication de probabilité ou de fiabilité. S'agissant du format, les aspects 'qualité' ont trait à l'inclusion d'un niveau de classification, de la date de l'échange, de la désignation du ou des service(s) partenaire(s) destinataire(s) et des réserves quant à l'utilisation ultérieure des données. Les cinq organes de contrôle peuvent tous contrôler la qualité de l'échange de données à cet égard.

La qualité peut également avoir une signification différente. Elle peut se rapporter à l'efficacité ou à l'efficience : l'échange de données est-il pertinent ? A-t-il eu lieu en temps voulu ? L'objectif est-il atteint ? Ce genre de contrôle de qualité est moins courant dans le chef des organes de contrôle. Les organes de contrôle belge et suisse sont expressément autorisés à vérifier l'efficacité et l'efficience d'un échange de données.

Révision du système d'échange de données dans son ensemble

Les organes de contrôle peuvent adopter une approche plus large lorsqu'ils contrôlent la légitimité d'un échange de données. En contrôlant certains cadres de coopération multilatéraux, l'organe de contrôle néerlandais a spécialement examiné le système d'échange de données dans son ensemble et la protection des droits individuels au sein même du système. Si certains échanges de données spécifiques peuvent être légitimes, le système peut malgré tout ne pas offrir de garanties suffisantes permettant d'assurer la légitimité de l'échange de données à plus long terme. Ce genre de contrôle peut contribuer à éviter un échange illégal de données entre les services de renseignement et de sécurité.

Une approche similaire pourrait être adoptée lors du contrôle de la qualité de l'échange de données. Lorsque l'objectif visé par l'échange de données est de contrer le djihadisme, la qualité générale de l'échange de données pourrait être mesurée en examinant la quantité d'informations partagées qui ont mené aux poursuites et à la condamnation, voire à directement à la prévention d'une attaque. Mais mesurer l'utilité des données échangées de cette manière peut s'avérer compliqué. Ce genre de contrôle est souvent mis en œuvre après la survenance d'un acte terroriste. L'organe de contrôle évalue alors si les données pertinentes ont été suffisamment et correctement échangées avec des partenaires nationaux et internationaux. L'organe de contrôle belge a été impliqué dans ce genre de contrôle.

Implication dans des recours et plaintes individuels

De manière générale, les organes de contrôle des cinq pays peuvent recevoir des plaintes concernant les activités des services de renseignement et de sécurité. Les organes de contrôle peuvent généralement rendre des avis ou des recommandations juridiquement non contraignants aux services renseignement et de sécurité et/ou aux ministres qui endossent la responsabilité politique. Les services respectent habituellement de tels avis

avis ou recommandations. Une nouvelle loi a été adoptée aux Pays-Bas en 2017, conférant à l'organe de contrôle le pouvoir de prendre des décisions contraignantes concernant les plaintes, y compris la possibilité d'ordonner la cessation de l'exercice d'une compétence ou encore la destruction ou le retrait des données traitées.

Le secret, qui est indispensable aux services de renseignement et de sécurité pour mener leurs activités, limite en général le droit des personnes à accéder à leurs données à caractère personnel. Certains pays accordent aux personnes le droit de demander à l'organe de contrôle national de vérifier les données à caractère personnel que les services ont traitées à leur propos. Au Danemark, quiconque peut demander à l'organe de contrôle danois de vérifier si le service de sécurité traite illégalement des données à caractère personnel le concernant. Dans le cas du service de renseignement militaire, ce contrôle est limité aux personnes résidant au Danemark. Dans les deux cas, l'organe de contrôle danois peut ordonner l'effacement des données relatives au requérant.

En Belgique, l'organe de contrôle a l'obligation d'examiner toutes les plaintes qui ne sont manifestement pas non fondées. Le plaignant recevra les conclusions de l'enquête formulées en termes généraux. Le plaignant aura alors la possibilité d'utiliser ces conclusions devant le tribunal ou une autorité administrative. Dans certains cas spécifiques, l'organe de contrôle doit rendre un avis officiel à une cour pénale à la suite d'une plainte. Par ailleurs, le comité peut prendre des décisions contraignantes concernant deux autres objets de plaintes que sont l'utilisation de méthodes particulières et la protection des données.

En Norvège, les résidents peuvent introduire une plainte auprès de l'organe de recours si un citoyen ou une citoyenne suspecte qu'il/elle a fait l'objet d'une surveillance illégale. Cependant, l'organe de contrôle norvégien n'a pas le pouvoir d'ordonner l'effacement des données. En Suisse, le Préposé Fédéral à la Protection des Données et à la Transparence (PFPDT) gère les demandes individuelles de traitement des données.

4. Défis du contrôle des échanges internationaux de données

En cours de projet, nous avons découvert que la coopération renforcée entre les services de renseignement et de sécurité et les échanges de données entre les services, en particulier au niveau multilatéral, peuvent poser des défis légaux et pratiques aux organes de contrôle.

Le contrôle ne traverse pas les frontières nationales

La législation nationale encourage souvent la coopération et les échanges d'informations entre les services de renseignement et de sécurité, tant au niveau bilatéral que multilatéral. Toutefois, elle ne prévoit généralement pas une base légale spécifique à l'intention des organes de contrôle pour coopérer ou échanger des informations sur des personnes. Aucun des cinq organes de recours collaborant dans le cadre de cette publication commune ne dispose d'une base légale explicite pour échanger des données avec un autre organe de contrôle, certainement pas lorsqu'il s'agit d'informations classifiées.

Les services de renseignement et de sécurité traversent les frontières, ce que ne peuvent pas faire les organes de contrôle. Le contrôle se limite aux mandats nationaux. Ceci reflète un aspect de l'échange de données : soit le contrôle se concentrera sur la communication de données et leur collecte préalable, soit il se concentrera sur la réception des données et leur utilisation. Les organes de contrôle nationaux ne seront pas en mesure, chacun de leur côté, d'avoir une vue d'ensemble sur l'échange de données à caractère personnel, sans parler du contrôle de la légalité ou du processus d'échange complet.

Une telle limite au contrôle national ne constitue pas nécessairement une lacune dans le contrôle. Lorsque le contrôle est exhaustif et efficace des deux côtés de la frontières, il n'y a pas de lacune dans les mandats des organes de contrôle. Cependant, quand il s'agit de la coopération entre les services de renseignement et de sécurité – principalement la coopération multilatérale – la coopération des organes de contrôle n'est jamais aussi solide que son maillon le plus faible.

Le défi de la coopération au regard du secret

Les organes de contrôle sont limités aux règles nationales régissant le secret et ne peuvent ni partager ni discuter de la substance de leurs enquêtes au-delà de ce qui est considéré comme information publique. Dans la pratique, cela signifie que les organes de contrôle ont une vue très limitée sur un éventuel contrôle efficace des échanges de données ou sur d'éventuelles lacunes en matière de contrôle. Les organes de contrôle ne peuvent pas traverser les frontières, pas plus qu'ils ne peuvent partager avec d'autres organes de contrôle ce qui se passe à intérieur de leurs frontières.

Au fil de la progression du projet commun aux cinq organes de contrôle, nous avons eu à maintes reprises l'occasion de nous rendre compte que nous n'étions même pas en mesure de discuter de questions connues de nous tous, par exemple, le contenu des accords conclus entre les services soumis à notre contrôle. En outre, nous avons réalisé que ce qui relève de l'information publique dans un pays pourrait être considéré comme confidentiel dans un autre pays. Notre projet s'en est trouvé compliqué, limitant les possibilités de mener une discussion substantielle sur ce point.

Évaluation de la nécessité et de la proportionnalité

Comme mentionné ci-dessus, les organes de contrôle évaluent en permanence la nécessité d'un échange de données pour atteindre un objectif spécifique, et ce, dans le respect du principe de proportionnalité. Pour ce faire, les organes de contrôle doivent tenir compte du niveau de protection des droits individuels accordé par le service qui reçoit les données. Avec l'augmentation du volume des échanges de données et du nombre de services étrangers avec lesquels les données sont échangées, les organes de contrôle seront confrontés à une tâche de plus en plus ardue. Ces critères de nécessité et de proportionnalité peuvent devenir plus abstraits et perdre de la valeur si les données échangées perdent en spécificité ou si elles sont échangées au sein d'un groupe plus large de services de renseignement et de sécurité.

Différents régimes juridiques nationaux peuvent inclure différentes normes de légalité et de qualité en matière de collecte, de traitement, de conservation et d'échange des données. Le degré de protection des droits individuels offert par le service qui reçoit les données est un élément important dans l'évaluation de la proportionnalité d'un échange de données particulier. Ce degré de protection n'est pas toujours aisé à déterminer, étant donné que les services de renseignement et de sécurité peuvent ne pas être ouverts sur tous les aspects du cadre légal en vigueur et sur les normes qu'ils appliquent.

Dans le contexte d'échanges de données multilatéraux, des normes et des définitions communes pourraient contribuer à définir dans quelles circonstances l'échange de donnée est considéré comme nécessaire et proportionnel et quel niveau minimal de protection des droits doit être mis en place pour offrir une garantie suffisante de respect des droits individuels. Il y a un intérêt commun pour toutes les parties – les services de renseignement et de sécurité et les organes de contrôle – à disposer de telles normes communes et d'une interprétation commune des garanties juridiques existantes. La légitimité des échanges multilatéraux dont il est question peut également s'en trouver accrue.

Distinction opérée par certains pays entre les citoyens et les étrangers

Certains cadres légaux nationaux offrent un niveau plus élevé de protection et un accès privilégié à des voies de recours individuels aux nationaux/résidents qu'aux étrangers/non-résidents. La distinction entre ces groupes peut limiter voire interdire l'accès à des recours individuels pour les étrangers ou non-résidents dont les données ont été échangées par les services de renseignement et de sécurité respectifs.

Une distinction similaire peut déterminer le mandat de l'organe de recours. Certains organes de recours ne sont mandatés que pour contrôler les échanges de données relatifs aux nationaux et résidents. La communication de données concernant d'autres personnes peut demeurer hors de leur portée. Si aucun autre organe de contrôle ne peut contrôler efficacement cette partie de l'échange de données, il en résulte une lacune dans le contrôle.

Moyens et méthodes d'échanges de données

Les services de renseignement et de sécurité échangent des données de différentes manières. Certains moyens et certaines méthodes d'échange de données sont autant de nouveaux défis pour les organes de contrôle. Entre autres exemples, citons l'échange informel de données, la manière de contrôler efficacement les données échangées lors de conférences et de réunions ou encore par téléphone. L'accroissement des échanges de données au niveau international peut contraindre les organes de contrôle à trouver des méthodes de contrôle plus perfectionnées. En effet, il ne leur est plus possible de contrôler chaque échange de données. En ce qui concerne la protection des données, les évolutions en matière d'échange de données au niveau multilatéral peuvent invoquer la responsabilité de chaque service participant, mais aussi des organes de contrôle. Pour offrir une garantie suffisante de respect des droits individuels, les services de renseignement et de sécurité pourraient être amenés à discuter des normes à appliquer et œuvrer à la définition d'un seuil minimal de protection commun à tous les services participants.

5. Vers un contrôle plus performant des échanges internationaux de données

Notre projet nous a montré que les efforts déployés par les services de renseignement et de sécurité pour trouver de nouveaux moyens d'échanger des données de manière efficace, en particulier au niveau multilatéral, et la forte augmentation du volume de données échangées, ont posé de nouveaux défis aux organes de contrôle. Sont autant concernés les limites des mandats nationaux des organes de contrôle, leur incapacité à discuter de manière appropriée des échanges internationaux de données avec d'autres organes de contrôle, que leurs propres efforts visant à innover leurs procédures et leurs méthodes en vue de garantir un contrôle efficace.

La souveraineté et les intérêts nationaux régissent la coopération internationale entre les services de renseignement et de sécurité. Contrairement à d'autres domaines de coopération internationale, il faut s'attendre à ce que le contrôle des services de renseignement et de sécurité continue à être exercé par les organes de contrôle nationaux.

Toutefois, les services de renseignement et de sécurité traversent les frontières, ce que ne peuvent pas faire les organes de contrôle. Le contrôle donc reflète toujours une face de l'échange de données. En outre, les organes de contrôle sont pour la plupart dans l'incapacité de partager leur contrôle sur un échange de données particulier avec d'autres organes de contrôle. Les limites du contrôle national font courir le risque de l'apparition de lacunes dans le contrôle en matière d'échange international de données par les services de renseignement et de sécurité. La question reste de savoir comment répondre à un tel risque.

Les organes de contrôle peuvent se rapprocher en échangeant des connaissances, des expériences et des méthodes d'enquête, mais aussi en comparant leurs constatations, conclusions et recommandations. C'est précisément ce que ce projet commun nous permis d'expérimenter. Nous avons appris de nos meilleures pratiques respectives, nous avons développé une meilleure compréhension de nos systèmes juridiques respectifs et nous avons instauré un certain climat de confiance. Afin de permettre aux organes de contrôle de suivre les développements de la coopération entre les services de renseignement et de sécurité, nous n'avons d'autre choix que d'intensifier notre coopération.

Une étape utile et nécessaire vers une coopération plus étroite est de limiter le secret lorsqu'il s'agit de partager des informations entre organes de contrôle. Ceux-ci devraient au moins pouvoir discuter des accords de coopération concrets qui ont été conclus tant au niveau bilatéral que multilatéral entre les services de renseignement et de sécurité soumis à leur contrôle. En toute logique, une étape supplémentaire pourrait être de partager des informations avec d'autres organes de contrôle qui ont déjà été partagées par les services de renseignement et de sécurité eux-mêmes. Une fois que les données ont été échangées, le contrôle peut être effectué dans la foulée. Nous ne suggérons pas que toutes les restrictions en matière de secret soient balayées d'un revers de main. Loin s'en faut. La coopération entre les organes de contrôle doit s'organiser dans les limites des normes établies par les législateurs nationaux.

Pouvoir discuter des accords de coopération internationaux et des échanges de données avec d'autres organes de contrôle implique certaines responsabilités. Offrir des garanties suffisantes de respect des droits individuels dans le cadre de la coopération internationale requiert que les services de renseignement et de sécurité discutent des normes qu'ils appliquent et œuvrent à la définition d'un seuil minimal de protection commun à tous les services participants. Cela requiert également que les organes de contrôle fassent respec-

ter ce seuil minimal de protection des données et tentent de trouver un terrain d'entente dans l'interprétation des garanties juridiques existantes.

Compte tenu des évolutions technologiques et du renforcement de la coopération, les échanges de données entre les services de renseignement et de sécurité s'intensifient, avec comme corollaire une augmentation du nombre d'échanges individuels de données. Le volume considérable de données échangées peut devenir un défi en soi. Évaluer la légitimité et la qualité de chaque échange individuel peut devenir une tâche écrasante pour les organes de contrôle. En plus des vérifications ponctuelles, il devient de plus en plus important d'évaluer le système et le cadre des échanges de données, ainsi que l'existence et le fonctionnement des garde-fous en matière de respect des droits fondamentaux.

Dans un souci d'efficacité, les organes de contrôle devront élaborer de nouvelles méthodes. Éventuellement en recourant de plus en plus à l'autonomisation informatique et à des outils développés pour contrôler de grands volumes de données. Pour ce faire, les organes de contrôle ont besoin d'étendre leur expertise en technologies de l'information et leur connaissance des systèmes utilisés par les services. Une autre manière de faciliter un contrôle plus efficace serait de prendre en considération les besoins des organes de contrôle lorsque les services mettent de nouveaux systèmes en place et de renforcer les mécanismes de contrôle interne et externe.

Les organes de contrôle belge, danois, néerlandais, norvégien et Suisse continueront à échanger leurs méthodes et leurs meilleures pratiques. Ils continueront à discuter des défis internationaux auxquels ils sont confrontés et des meilleures approches pour les relever. Nous invitons les organes de contrôle d'autres pays à se joindre à nos efforts pour limiter le risque de lacunes dans le contrôle et pour améliorer le contrôle des échanges internationaux de données entre les services de renseignement et de sécurité.

Signé à Berne le 22 octobre 2018

Mr. Serge Lipszyc, Président du Comité de contrôle des services de renseignements et de sécurité

Mr. Michael Kistrup, Président de l'Organe de contrôle des services de renseignements

Mr. Harm Brouwer, Président du Comité de contrôle des services de renseignements et de sécurité

Mrs. Eldbjørg Løwer, Présidente du Comité EOS – Le Comité de contrôle parlementaire des services de renseignements

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

De gauche à droite : Harm Brouwer (Président du CTIVD, Pays-Bas), Thomas Fritschi (Directeur de l'OA_IA, Suisse), Eldbjorg Lowe (Présidente du Comité EOS, Norvège), Serge Lipszyc, Président du Comité permanent R, Belgique.
Michael Kistrup, Président de l'Organe de contrôle du Danemark, n'a pu être présent quand cette photo a été prise.