Strengthening oversight of international data exchange between intelligence and security services

Written in cooperation between:

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. Content

Five European intelligence oversight bodies have begun a new form of cooperation.
In this statement, we will:

Describe our project, which entailed each of us conducting an investigation into our respective countries' services' use of information regarding foreign terrorist fighters and sharing our methods, best practices and experiences.

- Address the challenges we met when overseeing international data exchange, including the risk of an oversight gap when intelligence and security services cooperate internationally.

- Identify ways to move forward towards strengthening oversight cooperation, for example through minimizing secrecy between oversight bodies so that certain information can be shared, in order to improve our oversight of international data exchange.

2. Introduction

Recent terrorist attacks, such as in Paris, Brussels and London, were carried out by persons directed, encouraged or inspired by ISIS, Al-Qaeda or similar terrorist groups. To identify and investigate the threat of homegrown and returning foreign terrorist fighters is an important task for intelligence and security services across Europe.

The threat of jihadist terrorism has become more complex and widespread in recent years. Investigating this threat requires international cooperation between intelligence and security services, either bilaterally or multilaterally. Such cooperation exists within Europe and with other countries. As this cooperation has intensified, the exchange of personal data between services has increased. The exchange of data with foreign services is part of the intelligence and security services' day-to-day activities. Data may be exchanged in various ways, either orally or in writing.

The oversight bodies have naturally followed the development of international cooperation between intelligence and security services. As our respective oversight mandate is strictly national, we have been concerned with the risk of an "oversight gap" occurring. In an ideal situation, the national systems of oversight would be complementary to each other: where one oversight body reaches the boundaries of its national mandate, the other is competent to effectively oversee. However, national legislation regarding exchange of data and the oversight of such exchanges may not meet these requirements. Moreover, international cooperation between intelligence services could develop in such a way, that national oversight can no longer keep up. Then an "accountability deficit" or "oversight gap" could emerge.

In light of this, the five oversight bodies from Belgium, Denmark, the Netherlands, Norway and Switzerland decided to start a joint project to exchange experiences and methods. Each of the oversight bodies conducted a national investigation into the international exchange of data on foreign terrorist fighters by the intelligence and security services they oversee.[1]

We conducted the national investigations more or less at the same time, each from our national context and within the framework of our national mandate. We have met regularly to compare investigation methods, interpret legal frameworks, discuss legal and practical problems and to collate our findings and conclusions. Classified information was not exchanged.

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

3. Current practices in oversight of data exchange

The participating oversight bodies oversee data exchange between intelligence and security services in several ways. We may

- assess cooperative relations or arrangements between intelligence and security services,
- assess the legitimacy and quality of specific data exchanges with foreign services,
- review the system of data exchange as a whole, including the safeguards,
- be involved in procedures concerning individual remedies and complaints.

Although the mandates of the oversight bodies are different, we all have a diverse range of instruments for overseeing international data exchange.

Assessment of the cooperative relationship

Oversight bodies may assess whether or not the cooperative relationship between their country's service and partner services in other countries meets certain criteria. Legislation governing the intelligence and security services may specifically state criteria for cooperation. Typically, criteria include the necessity for cooperation, the respect for human rights, the existence of legislation on data protection and/or reliability. The threshold for cooperating with services that do not meet the criteria should be high. The oversight bodies of Belgium, the Netherlands, Norway and Switzerland review the considerations made in that respect by their national services.

Cooperative relationships between the services can be based on agreements, for example letters of intent or memorandums of understanding. Such agreements are usually not legally enforceable but offer a practical framework on the exchange of data by services. Even the existence of some of these agreements is classified. Other agreements are made public by governments or the services. Nevertheless, they may draw the outline of the cooperative relationship by addressing issues like the purpose of the cooperation, how the cooperation is expected to function, limitations concerning disclosure to third parties or procedural aspects of the cooperation. The oversight bodies of all five countries may either review or report on whether these agreements comply with national laws and regulations.

Assessment of the legitimacy of specific data exchanges

Oversight bodies may assess whether individual data exchanges meet the legal requirements imposed by national laws and regulations.

The national legislations of our countries share certain characteristics, most notably the principles of necessity and proportionality. These shared principles originate from international legal frameworks such as the European Convention on Human Rights. The principle of necessity includes the requirement of a clear and legal purpose for the data exchange and the reasonable expectation that this purpose will be

met by exchanging the data. The principle of proportionality requires the service to balance the purpose of the exchange against the gravity of the infringement of fundamental rights. Most national legislation contains other requirements as well, such as the reasonableness, correctness, effectiveness and reliability of data exchange.

The internal policy of the services may provide additional rules for data exchange. Such policy may, for example, further specify which type of data exchange is allowed under which circumstances, which authorisation level is required and which use may be made of data received. When national law or bilateral and multilateral agreements are absent or silent on a specific matter, internal policy can provide additional safeguards.

Assessment of the quality of specific data exchanges

Quality may relate to the content of the data or the format of the data. When it comes to content, quality means the data is correct, sufficiently clear and precise in its wording, confirmed by underlying data, up to date and with an indication of probability or reliability. As for format, quality aspects relate to the inclusion of a classification level, the date of exchange, the designated receiving partner service(s) and caveats regarding further use of data. All five oversight bodies can review the quality of data exchange in this respect.

Quality may also have a different meaning. It may relate to efficiency or effectiveness, that is whether the data exchange is relevant, whether the exchange happened in a timely manner and whether it fulfilled its purpose. This type of quality review is less common for oversight bodies. The oversight bodies of Belgium and Switzerland are expressly authorised to review whether data exchange has been effective and efficient.

Review of the system of data exchange as a whole

Oversight bodies may adopt a broader approach when reviewing the legitimacy of data exchange. In reviewing certain multilateral cooperative frameworks, the oversight body in the Netherlands expressly looks at the system of data exchange as a whole and at the protection of individual rights within that system. Even though certain specific data exchanges may be legitimate, there can still be insufficient safeguards in the system to ensure the legitimacy of data exchange in the longer run. This type of review may help prevent unlawful data exchange between intelligence and security services.

One could take a similar approach when reviewing the quality of data exchange. When the purpose of exchanging data is to counter jihadism, the general quality of data exchange could be measured by investigating the amount of shared information that led to prosecution and conviction, or even to a direct prevention of a terrorist attack. However, measuring the usefulness of exchanged data in this way can be challenging. Such reviews are often initiated after a terrorist attack has occurred. Then the oversight body assesses if the relevant data had sufficiently and adequately been exchanged with national and international partners. The oversight body of Belgium has been involved in this type of review.

Involvement in individual remedies and complaints

In general, oversight bodies in all five countries can receive complaints from individuals regarding the activities of the national intelligence and security services. Usually oversight bodies may offer non-legally binding opinions or recommendations to the intelligence and security services and/or the ministers who are politically responsible. The services usually comply with such opinions or recommendations. A

new law was adopted in the Netherlands in 2017, granting the oversight body the power to take binding decisions on complaints. This may also include ordering the exercise of a power to be terminated or the destruction or removal of processed data.

The secrecy that is necessary for the intelligence and security services to conduct their activities usually limits the right of the individual to access personal data. Some countries explicitly afford individuals the right to request the national oversight body to review the personal data their services have processed about them. In Denmark, any person may ask the Danish oversight body to investigate whether the security service is unlawfully processing personal data about them. In case of the military intelligence service, this review is limited to residents of Denmark. In both cases, the Danish oversight body may order the deletion of personal data regarding the applicant.

In Belgium the oversight body has an obligation to investigate all complaints that are not manifestly unfounded. The complainant will receive the findings of the investigation in general terms. The complainant then has the possibility to use these findings before the court or an administrative authority. In some specific cases the oversight body must give an official advice to a criminal court following a complaint and regarding two other topics of complaint (use of special methods and data protection), the committee may take binding decisions.

In Norway, residents have the same right to complain to the oversight body if a citizen suspects that he/she is subject to unlawful surveillance. However, the Norwegian oversight body does not have the authority to order deletion of data. In Switzerland, the Federal Data Protection and Information Commissioner (FDPIC) handles individual requests on data processing.

4. Challenges for oversight of international data exchange

In the course of our project we have found that the increased cooperation between intelligence and security services and the exchange of data between these services, especially on the multilateral level, may pose legal and practical challenges to the oversight bodies.

Oversight does not cross national borders

National legislation often promotes the cooperation and exchange of information between intelligence and security services, both bilaterally and multilaterally. However, it usually does not provide a specific legal basis for oversight bodies to cooperate or exchange information on individuals. None of the five oversight bodies working together in the context of this common publication has an explicit legal basis to exchange data with another oversight body, certainly not when this information is classified.

Where intelligence and security services cross national borders, oversight bodies cannot. Oversight is limited to national mandates. This reflects one side of data exchange: either oversight will focus on the provision of data and its prior collection, or it will focus on the reception of data and its use. National oversight bodies will not independently be able to acquire a full picture of personal data exchange, let alone review the lawfulness of the entire process of exchange.

Such a limit to national oversight does not necessarily constitute an oversight gap. When oversight is exhaustive and effective on both sides of the border, no gap exists between the mandates of the oversight bodies. However, when it comes to cooperation between intelligence and security services - predominantly multilateral cooperation - the cooperation of oversight bodies is only as strong as its weakest link.

The challenge of cooperation in the face of secrecy

Oversight bodies are limited to national rules on secrecy and cannot share and discuss the substance of their investigations beyond what is designated as public information. In practice, this means that oversight bodies have very limited insight into whether 'the other side' of data exchange is effectively overseen or whether an oversight gap exists. Therefore, oversight activities are not only unable to cross borders; they are also largely unable to share with other oversight bodies what occurs within their borders.

As the joint project between the five oversight bodies progressed, we found ourselves on numerous occasions aware of the fact that we were not even in a position to discuss matters known to us all, e.g. the content of agreements between the services we oversee. In addition, we became aware that what is public information in one country might be deemed confidential in another. This has led to difficulties for this project, limiting the possibility to reach substantial discussion on the matter in question.

Assessment of necessity and proportionality

As mentioned above, oversight bodies continuously assess whether the exchange of data is necessary for a specific purpose and proportionate to the aim pursued. This requires that oversight bodies consider the level of protection of individual rights provided by the receiving service. As the volume of data exchanges and the number of foreign services with which the data is shared increase, this will be more and more challenging for oversight bodies. This test of necessity and proportionality can become more abstract and can lose value as the data exchanged is less specific or if it is exchanged within a larger group of intelligence and security services.

Different national legal regimes may include different legitimacy and quality standards for data collection, processing, retention and exchange. The level of protection of individual rights afforded by the service receiving the data is an important element in assessing the proportionality of a particular data exchange. This is not always easy to determine as intelligence and security services may not be open about all aspects of the legal framework in place and the standards they apply.

In the context of multilateral data exchange, common standards and definitions could help define under which circumstances data exchange is regarded as necessary and proportionate, and which minimum level of data protection needs to be in place to sufficiently safeguard individual rights. There is a common interest of all parties – intelligence and security services and oversight bodies – in having such common standards and a common interpretation of existing legal safeguards. This may also add to the legitimacy of the multilateral exchange in question.

Some countries differentiate between citizens and foreigners

Some national legal frameworks offer nationals or residents a higher level of protection and more privileged access to individual remedies than foreigners or non-residents. The distinction between these groups may result in limited or no access to individual remedies for foreigners or non-residents whose data has been exchanged by the respective intelligence or security service.

A similar distinction may determine the mandate of the oversight body. Some oversight bodies only have the mandate to review data exchange with regard to nationals or residents. The provision of data with regard to other persons may lie beyond their reach. If no other oversight body may effectively review this part of the data exchange, an oversight gap exists.

Means and methods of data exchange

Intelligence and security services exchange data in various ways. Some means and methods of data exchange pose further challenges for oversight bodies. An example of such a challenge is the informal exchange of data, and how to provide efficient oversight of data exchanged during conferences and meetings, by phone and so on. The increase in international data exchange may require oversight bodies to come up with more advanced methods of oversight, as it is no longer feasible to review each exchange of data. With regard to data protection, developments in multilateral data exchange may invoke responsibilities for each of the participating services as well as the oversight bodies. To safeguard individual rights adequately, it may be required that intelligence and security services discuss the standards they apply and work towards an equal minimum level of protection offered by all participating services.

5. Oversight of international data exchange – moving forward

Our project has shown us that the efforts of the intelligence and security services to find new ways to exchange data effectively, especially on a multilateral level, and the large increase in the volume of data exchanged, have in turn led to new challenges for the oversight bodies. This applies both to the limits of the oversight bodies' national mandates, their inability to adequately discuss international data exchange with other oversight bodies as well as to their own efforts to innovate their procedures and methods to ensure effective oversight.

National sovereignty and interests dictate the international cooperation between intelligence and security services. It is to be expected that, unlike other areas of international cooperation, oversight of the intelligence and security services will continue to be carried out by national oversight bodies. However, where intelligence and security services cross national borders, oversight bodies cannot. Consequently, oversight always reflects on one side of data exchange. Moreover, oversight bodies are largely unable to share with other oversight bodies their review of a particular data exchange. Because of these limits to national oversight, there is a risk of an oversight gap with regard to international data exchange by intelligence and security services. The question remains how to tackle such a risk.

By exchanging knowledge, experience and investigation methods, and by comparing their findings, conclusions and recommendations, oversight bodies may come closer together. Our experience is that this is precisely what this common project has accomplished. We have learned from each other's best practices, developed more understanding of each other's legal systems and we have built a level of trust. In order for oversight bodies to keep up with developments in international cooperation between intelligence and security services, we need to do just that: intensify our cooperation.

A valuable and necessary step towards closer cooperation is to minimize secrecy when sharing information between oversight bodies. At the minimum, oversight bodies could be able to discuss concrete bilateral and multilateral cooperative arrangements between the intelligence and security services they oversee. A logical additional step could be to share information with other oversight bodies that has already been shared by the intelligence and security services themselves. Once data has been exchanged, there is no need for oversight to lag behind. We do not suggest that all national secrecy limitations should be set aside, to the contrary. Cooperation between oversight bodies should take place within the limits and according to the standards set by national legislators.

Being able to discuss international cooperative arrangements and data exchange with other oversight bodies also comes with certain responsibilities. Adequately safeguarding individual rights while cooperating internationally, not only requires that intelligence and security services discuss the standards they apply and work towards an equal minimum level of protection offered by all participating services. It also requires oversight bodies to uphold such a minimum level of data protection and try to find common ground in interpreting existing legal safeguards.

Due to technological development and increased cooperation, the data exchange between intelligence and security services is intensifying, resulting in an increase of the number of individual data exchanges. The sheer volume of data exchanged may become a challenge in itself. To assess the legitimacy and quality of each individual exchange can become an overwhelming task for the oversight bodies. In addition to

conducting spot checks, it is becoming increasingly important to assess the system and framework for data exchange and the existence and functioning of safeguards for the protection of fundamental rights.

To do this effectively, oversight bodies will need to develop new methods. One way forward may be to increasingly use computerized automation and tools developed for conducting oversight of large volumes of data. In order to achieve this, oversight bodies need to expand their IT expertise and knowledge of the services' systems. Another way to facilitate a more effective oversight would be to take the needs of the oversight bodies into account when the services implement new systems and to strengthen mechanisms of internal and external control.

The oversight bodies of Belgium, Denmark, the Netherlands, Norway and Switzerland will continue to exchange methods and best practices, as well as discuss international challenges to oversight, and the best approaches to overcoming these challenges. We invite oversight bodies from other countries to join us in our efforts to limit the risk of an oversight gap and to improve oversight of international data exchange between intelligence and security services.

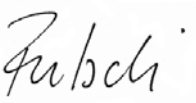
Signed in Bern on 22 October 2018,

Mr. Serge Lipszyc, Chair of the Belgian Standing Intelligence Agencies Review Committee

Mr. Michael Kistrup, Chair of the Danish Intelligence Oversight Board

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

Mrs. Eldbjørg Løwer, Chair of the EOS Committee – The Norwegian Parliamentary Intelligence Oversight Committee



Mr. Thomas Fritschi, Director of the Independent Oversight Authority for Intelligence Activities

From left to right: Harm Brouwer (chair CTIVD, the Netherlands), Thomas Fritschi (director OA-IA, Switzerland), Eldbjorg Lower (chair EOS Committee, Norway), Serge Lypszyc (chair Comité I, Belgium). Michael Kistrup, chair of the Danish oversight board, could not be present when this photo was taken.