Bridging the oversight gap in international collaboration between intelligence and security services

Mireille Hagens
IIOF – 29 November 2018

Introduction

Together with all of you here today, I would like to explore the urgent issue of strengthening cooperation between oversight bodies of intelligence and security services. Also I would like to share with you the experiences of the joint project on this issue that the Dutch Review Committee on the intelligence and security services, where I work as a senior review officer, undertook in collaboration with the oversight bodies of Belgium, Denmark, Norway and Switzerland.

In an interview published in March 2016 our esteemed colleague from New Zealand, Inspector-General of Intelligence and Security Cheryl Gwyn, also underlined the importance of this topic. She stated, and I quote from the article: "there is a gap in the intelligence world. Snowden revealed how closely the international spy agencies work together, but their oversight agencies can't do this." I still quote: "How do I know that what the intelligence agencies get from other jurisdictions is lawfully and properly sourced?", she asks. "And how do we know what use other jurisdictions put our intelligence to?" Unquote. The Inspector-General sees it as the ultimate solution to allow her and the Inspector-General of the CIA to carry out a joint investigation. The article ends with the powerful phrase, and I quote: "Watchdogs of the world unite."

In a nutshell, this is the challenge that all of the national oversight bodies of intelligence and security services currently face. And it is not only our responsibility to overcome this challenge but also that of the intelligence community itself. Let us now discuss in more detail the urgency of the oversight gap and the ways in which we can work together to bridge this gap.

Increasing collaboration intelligence community

Intelligence and security services increasingly work together in an international context on a wide range of issues, for instance to combat violent jihadism. This is essential to effectively address this cross-border, complex and diffuse threat. An example of a multilateral cooperative arrangement that developed at a high pace in recent years is the Counter Terrorism Group (CTG), a partnership of 30 European security services, being the services of the EU countries, Norway and Switzerland. There are also close multilateral collaborations in the field of signals intelligence (SIGINT).

On the issue of jihadist terrorism, the Dutch Review Committee conducted an investigation in 2017 into the multilateral cooperation of the Dutch General Intelligence and Security Service (AIVD) and specifically the exchange of personal data on foreign terrorist fighters, within the Counter Terrorism Group and within SIGINT-collaborations. Our review report was published in February of this year. It was translated into English and is available on our website.

Multilateral cooperation on this issue can take various, far-reaching forms. If we focus on the CTG, we see a rising level of mutual trust between the cooperating services. There is also

increasing mutual openness regarding the level of knowledge, the methods used and sometimes even regarding the means or sources used to obtain data. There is also a clear ongoing development aimed at sharing personal data more quickly and effectively and jointly storing and processing such data. Examples of this include the establishment of a joint database and an operational platform. The CTG database was activated on 1 July 2016 and is available in real time to all 30 services participating in the CTG. This means that if personal data of known or suspected jihadists is added to the database by one of the participating services, this data is almost immediately operationally accessible to the other participating services. This database runs on a server on Dutch territory.

The CTG operational platform, which is also based in the Netherlands, was formally opened in January 2017. It allows for more detailed multilateral operational consultations, through permanent physical presence of representatives of the participating services and regular operational meetings. Concrete, defined cases are discussed during these meetings of the platform.

Within the framework of other cooperative arrangements, even further steps are being taken. In that context investigatory powers are being jointly used and joint intelligence products are produced. This is not yet the case within the CTG, but this could be the reality of tomorrow.

These intensive and far-reaching multilateral partnerships entail a joint responsibility of the participating services. Under international law, each of them is responsible and each of the states of these services liable for the cooperation as a whole and the joint activities. The reason for this is, that the chosen forms of multilateral cooperation have an informal structure, meaning that they find their basis in national law and in mutual agreements between the heads of the participating services jointly. The cooperation is not regulated by formal, legally binding agreements, and lacks a formal division of responsibilities. Any violation of human rights and fundamental freedoms may thus lead to joint liability.

The intensification of multilateral cooperation between intelligence and security services is now of such a magnitude that it has potentially far-reaching implications for the individual. This requires sufficient safeguards for the protection of human rights, specifically common standards of data protection within the multilateral cooperative arrangements. It is the joint responsibility of the participating services to decide how to provide adequate legal protection and which safeguards must be addressed, elaborated and complied with. The Dutch Review Committee found that within the Counter Terrorism Group such common standards existed only to a limited extent.

In addition, it is also necessary that the legal safeguard of independent, adequate and effective oversight is provided for in a common framework for data protection within the multilateral cooperation. National oversight alone is not enough. This would mean that oversight of the existence of and compliance with common multilateral standards would be carried out by as many oversight bodies and jurisdictions as there are participating countries, with all their differences in organisation and powers. These oversight bodies would probably be limited to the contribution of the specific services they oversee. This seems unworkable and carries the risk that no one is overseeing the full functioning of the database and platform with all its effects. The oversight of joint responsibility for the existence and operation of common data protection standards calls for joint oversight.

Oversight gap

Let us explore the issue of joint oversight in more detail. Where the intelligence community is intensifying cooperation which has led to more, faster and larger volumes of data being exchanged between services in different countries, this poses a number of challenges for national oversight bodies, with the risk of an oversight gap occurring.

There are several reasons for this. Firstly, national legislation usually does not provide a specific legal basis for oversight bodies to cooperate. Oversight of international data exchange is therefore limited to national mandates. One way an oversight body can do this in the national context, is to assess whether or not the cooperative relationship between a country's service and partner services in other countries meets certain criteria. In the Netherlands this assessment is laid down in so called weighting notes. As national oversight cannot cross borders, it can as a consequence only reflect on one side of data exchange: either it will focus on the provision of data and its prior collection, or 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. When oversight is exhaustive and effective on both sides of the border, no gap exists between the territories of the oversight bodies. However, with all their differences in organisation, mandate and powers this is not the current situation.

Secondly, even if oversight bodies cooperate, they are largely unable to share with each other what occurs within their borders. They are limited by national rules on secrecy and cannot share and discuss the classified substance of their investigations. 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. The rules of secrecy extend to information that has already been exchanged between intelligence services and even to the mere notion that data exchange has taken place. The same applies to formal or informal agreements made between intelligence services. Sometimes the mere existence of such agreements is classified. This means that cooperating oversight bodies are not even in a position to discuss matters known to all of them, for instance the fact that information has been exchanged or the content of agreements between the services they oversee. Such agreements can be very important in providing safeguards for the protection of fundamental rights and should therefore be subject to oversight cooperation.

Thirdly, some oversight bodies only have the mandate to review data exchange with regard to nationals or residents. If no other oversight body may effectively review the provision of data with regard to other persons, an oversight gap exists.

Fourthly, oversight bodies are finding it more and more of a challenge to keep up with developments of the intelligence community towards increasing, faster and more effective ways of data exchange, for example during day to day cooperation within a joint platform, but also through the use of joint databases, the exchange of larger volumes of data (bulk), and new technological possibilities. This requires oversight bodies to think about the effectiveness of their oversight. Also the increase in data exchanges requires oversight bodies to come up with more advanced methods, as it is no longer feasible to review each data exchange.

The foregoing illustrates that the risk of an oversight gap is real. This poses a threat for international cooperation of intelligence and security services. International data exchange may be unlawful without the oversight community knowing about it. And, more importantly, the intelligence services run the risk of a national or international court declaring their cooperation unlawful. There is a real chance someone will bring a case to a court, say the

European Court of Human Rights. As the recent judgment in the case of Big Brother Watch and others versus the United Kingdom shows us, effective oversight is an important safeguard in determining the existence of sufficient checks and balances when it comes to activities of secret services. Should this happen, should a court review the existence of sufficient checks and balances for international cooperation, intelligence and security services may find themselves confronted with a serious legitimacy problem. Therefore, it is also in the interest of intelligence services to strengthen oversight cooperation or joint oversight as this provides legitimacy to their international cooperation. So, it is not only a task for oversight to find ways to more effectively oversee international intelligence cooperation, it is in the interest of the entire intelligence community.

Bridging the oversight gap

In light of this, the five oversight authorities from Belgium, Denmark, the Netherlands, Norway and Switzerland, started a joint project to address the challenges intensified international data exchange may pose to oversight and to identify ways to tackle the risk of an oversight gap. Each of the oversight bodies conducted, more or less at the same time, a national investigation into the international exchange of data on foreign terrorist fighters by the intelligence and security services they oversee. Over the last three years, the five oversight bodies have met regularly to compare investigation methods, interpret legal frameworks, discuss legal and practical problems and share experiences within the national investigations, without the exchange of classified information.

To bridge the oversight gap, cooperation between oversight bodies needs to intensify and become more effective. The joint project identified two ways forward.

Firstly, a valuable and necessary step towards closer and effective oversight collaboration is to minimize secrecy between oversight bodies. Once data has been exchanged by intelligence services and once agreements about their cooperation have been concluded, there is no reason for oversight to lag behind. This is not something that oversight bodies can tackle themselves. This needs to be addressed in national legislation. In the law it should be stated that oversight bodies are allowed to discuss classified information, provided that this information has already been exchanged by the intelligence services. Therefore it is important that each oversight body discusses this on the national level with parliaments and responsible ministers.

Being able to discuss international cooperative arrangements and data exchange between oversight bodies also brings certain responsibilities. The adequate safeguarding of individual rights during international cooperation, not only requires that the intelligence and security services discuss the common standards they apply and work towards an equal 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.

Secondly, another step forward is the development of new legal and technical methods of oversight, in order to effectively assess the system of international data exchange and the existence and functioning of common safeguards for the protection of fundamental rights.

Instead of focusing on the legitimacy and quality of each individual data exchange or conducting representative spot checks, which can become an overwhelming task, it is becoming increasingly important to assess the system and framework for data exchange and the safeguards within this system. This is more or less a risk assessment and constitutes a

different legal method for conducting oversight. Even where most individual data exchanges up to now may be legitimate, there can still be insufficient safeguards in the system to ensure the legitimacy and quality of data exchange and processing in the longer run. Pinpointing risks or weaknesses where it comes to safeguards, may lead to a strengthening of those safeguards by intelligence services. It may also provide oversight bodies with a better scope, to determine more precisely the focus of their review.

In addition, oversight bodies will need to develop new technical methods and share with each other best practices on oversight innovation. This includes strengthening their own technical expertise, using automated forms of oversight, for instance using data analyses to find anomalies in data processing or data exchange, and ensuring that within the services sufficient internal control and compliance mechanisms are in place that can contribute to effective external oversight. Focusing more on the technical systems and processes of the intelligence services could largely improve the quality and effectiveness of oversight. As this is no easy task, it is beneficial to all of us oversight bodies to share our experiences and learn from each other's efforts.

Conclusion

That brings me to the conclusion of my speech. The resounding success of multilateral cooperation between security services in Europe in recent years also has its pitfalls. They are found in the lack of adequate legal protection for individuals and limitations for effective oversight. This entails the risk of an oversight gap, which in its turn poses a danger for international cooperation between intelligence and security services. It is not only in the interest of oversight to strengthen the cooperation of oversight bodies, it is also of importance to the intelligence community to ensure the legitimacy of their international cooperation.

For us as oversight authorities, it is important that we strive to overcome the various difficulties oversight of international intelligence cooperation presents. As our joint project illustrates, oversight cooperation is a challenge and takes time. But with a successful first project, we shall continue our approach and we hope other oversight bodies will join us in our efforts to strengthen oversight cooperation.

Thank you for your attention.