Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

Challenges for effective oversight

Speech for Paris conference 7 December 2018

Avant tous!
Mesdames et messieurs,
C'est pour moi un grand honneur de pouvoir prendre la parole à l'occasion de cette conférence organisée par la Commission Nationale française de Contrôle des Techniques de Renseignements et par le Comité permanent de contrôle des services de renseigement et de securité belgique. Etre ici et rencontrer autant de collègues européens est une expérience enrichissante. Je remercie infiniment Francis Delon, Guy Rappalle et Sèrge Lypzics d'avoir pris l'initiative d'organiser cet évènement, qui nous donne à tous la possibilité d'approfondir nos relations.

Please allow me to continue in English. My name is Harm Brouwer, and I am the chair of the Dutch Review Committee on the Intelligence and Security Services, better known as the CTIVD. During this presentation I would like to talk to you about the challenges for effective oversight in the reality of operational intelligence, characterized these days not only by increasing threats for national security, amongst others, in terms of cyber-attacks, espionage and violent jihadism, but characterized also by technological innovations, and the intensifying multilateral cooperation between the services themselves.

Developments

We have entered a new era, that evolves around hugely intensified data exchange and data processing. Organizations like Amazon, Apple, Facebook, Google and Microsoft more and more determine the digital world we live in today. Data has become a commodity, a new currency. Large amounts of data are continuously exchanged and processed, without us knowing or understanding what this actually entails and what this is used for.

Current technological developments also provide both huge opportunities as well as challenges for the intelligence and security services we oversee. A notion that is shared across nations in Europe and beyond. In multiple European countries, national legislation governing the powers of intelligence and security services has been recently changed, partly because of these technological developments. In the Netherlands this has taken place as well. A new Intelligence and Security Services Act entered into force on the first of May 2018, expanding the special powers of the services to be able to collect and process large amounts of data, both ether and cable-bound data, in various ways. Such legislative developments are of vital interest to the protection of national security.

Bulk interception powers are legally accepted, which has been confirmed in the recent judgments in the Rättvisa and Big Brother Watch cases by the European Court of Human Rights. What these judgments also make clear is that from the perspective of the protection of individual rights, it is essential that the extension of powers of the intelligence and security services goes hand in hand with adequate safeguards against abuse and with safeguards for effective oversight.

International cooperation between intelligence and security services adds another dimension to the availability of large volumes of data. This international cooperation has assumed considerable proportions in recent years, with a tendency towards exchanging more and more unevaluated data in bulk. Also, there are multilateral developments towards the joint deployment of special powers, joint storage of data, joint data processing and the subsequent joint production of intelligence products. While this intelligence cooperation is justifiably intensive and far-reaching, it also has implications in terms of legal protection for individuals and for effective oversight.

So in essence, intelligence and security services more and more have the possibility of collecting large volumes of data in bulk, by its nature most of which related to persons that do not require the interest of the intelligence services. The automated filtering, analyses, selection and other steps of processing of such data are therefore imperative to making a distinction between data that is relevant and data that is not and should be destroyed as soon as possible. Complex automated processes which are not easy to review.

Effective oversight

What does this all mean for effective oversight? How do national oversight bodies keep pace with these developments and make sure that they do not lag behind the intelligence and security services they have to oversee? In my opinion there is no single solution for accomplishing effective intelligence oversight in the present digital era. What might be, however, is a shared understanding that oversight bodies need to innovate, that they must adapt to a changing intelligence context and that they can and should learn from each other.

So what does this all mean for effective oversight?

Firstly, oversight bodies should strengthen their technical expertise. Where traditionally, oversight is built around legal experts assessing the legality of the activities of the intelligence and security services, this seems no longer feasible without understanding the underlying supporting technical processes that are taking place on a day to day basis. Effective oversight requires the involvement of IT architects, cyber specialists, data scientists and so on. But it is by no means an easy task to find the right people for those jobs and to determine what exactly it is, that they should undertake. Several years ago, our first step in strengthening our technical expertise, was to set up a so called knowledge network of renowned legal and technical scientists of different universities, for brainstorming and feed-back purposes. This network provides us with advice and acts as a sounding board in our investigations. The members of this network all have high

security clearances from the services. We have also focused on recruiting researchers with both an ICT and law background, legal experts with a good technical understanding. But most importantly, over the past few years, the CTIVD has built up a small IT unit. This unit has turned out to be a very valuable expansion of our staff. We are gradually conducting more technical investigations, necessary for effective oversight for instance in the field of compulsory permanent data reduction, but it is still somewhat trial and error. We are not yet as effective in our oversight as we would like to be, but we are well underway.

So what does this all mean for effective oversight?

Secondly, oversight bodies should not only have full and direct access to the systems of the services, they should also, based on that provision, focus more on safeguards for the ways in which data is processed, in all phases of data processing. This requires paying more attention to throughput, instead of only assessing the authorization in advance for the exercise of powers and the outcome of that exercise. National legislation as well as the jurisprudence are often focused on ex ante binding oversight, meaning strict authorization requirements and procedures prior to data collection. Whereas this is an important safeguard, national legislation should also provide oversight bodies with adequate powers and tools to critically review the automated filtering, analyses, selection and other steps in the processing of the large volumes of data that are being collected. Because it is a matter of fact, that the largest infringement of privacy does not occur in the authorization phase but during the actual processing and use of the collected data. National legislation should therefore also require the services to implement, for the sake of compliance, generally accepted internal control mechanisms which can be externally overseen.
In the Netherlands such a requirement was added to the law in terms of a so called duty of care for the legality and quality of data processing. This duty of care creates the obligation for the services to design their internal processes and systems according to the general principles of data protection such as data protection by design and by default, to conduct risk analyses and to have internal control mechanism in place, such as audits. All to be implemented in a way that adequate and effective oversight or review is possible.

For example, when it comes to automated data analyses, it is important to understand the working of particular algorithms and models. It is essential to check whether such algorithms and models are tested before their application and whether the services continuously exercise internal control on their proper functioning. Focusing more on the technical systems and processes of the intelligence services, could largely improve the quality of oversight. It may also improve the span of control of oversight. The needs of oversight could already be taken into consideration when services implement new systems, in which mechanisms of internal and external control can be strengthened. A legal requirement for the services to report the introduction of new techniques is a valuable instrument in this regard. I believe the French CNCTR sets an example of best practice here. And when it comes to reviewing internal control mechanisms the methods of het Danisch oversight board may well serve as a model.

So what this all mean for effective oversight?

Thirdly, it is important that oversight bodies share with each other the ways in which they seek oversight innovation, so they can learn from each other's efforts and best practices. In this respect, I would like to mention the already existing cooperation between five oversight bodies, from Belgium, Denmark, the Netherlands, Norway and Switzerland. We have issued a joint statement last month, addressing the challenges for national oversight when it comes to reviewing international data exchange. The statement noted that there is a risk of an oversight gap, also referred to as the 'accountability deficit'. National oversight bodies can only reflect on one side of data exchange, they cannot on their own review all aspects of intelligence exchange. Cooperation between oversight bodies, which can fill the gap, is hindered by the obligation of obtaining secrecy towards each other.
Oversight cooperation, however, is becoming increasingly important. Not only in sharing best practices, but also in assessing together the existence and functioning of safeguards for the protection of fundamental rights within the multilateral cooperative frameworks the services work with these days. This requires oversight bodies to uphold together a minimum level of protection within those multilateral frameworks and to find common ground in interpreting existing legal safeguards. Strengthening oversight cooperation is therefore a high priority for us and we invite you to join us in our efforts, us that is the existing cooperation between the five European intelligence oversight bodies.

Conclusion

Which brings me to the conclusion of my presentation. We are all confronted with the realities of an operational intelligence, characterized by increasing threats for our national security, by technological developments and by intensifying intelligence cooperation. Intelligence and security services more and more have the possibility of collecting, analyzing and using paramount volumes of data. In order to remain effective in our work, we need to adapt to this reality. We need to strengthen our technical expertise, focus more on safeguards for the ways in which data is processed and share with each other the ways in which we seek oversight innovation. It is not clear yet, in all stages of development, how exactly we can accomplish this important task that lies before us. However, it is evident that we need to innovate, that we need to keep pace with technological and international developments, that we can and should learn from each other and therefore should intensify our cooperation.

Dear collegues,

The CNCTR and the Permanent Committee R took an important step in bringing us all together here in Paris. The CTIVD much values this initiative and finds it of great importance to continue on this road. I therefore would like to announce, as a host, that a next conference of European intelligence oversight bodies will be organized to take place in The Hague in the Netherlands in the second half of June 2019. We will make sure to extend an invitation to all of you here present, shortly.

Thank you for your attention.