International Intelligence Review Agencies Conference, 8 July 2014, London
Speech by Mr. Harm Brouwer
Chairman of the Dutch Review Committee for the Intelligence and Security Services

A call for more transparency:
A Dutch perspective on large scale intelligence gathering and international cooperation

Opening words

The year 2013 placed a strong spotlight on the intelligence community. Fundamental questions were asked about the ethics of large scale intelligence gathering. In the slipstream of this discussion. I would like to share with you the main findings of the Dutch Review Committee's investigation in response to Parliamentary questions following the Snowden-allegations.

Introduction

The Netherlands ranks year after year as one of the nations with the widest use of internet and social media. This means that a large proportion of social interaction takes place online. Also, the Netherlands has a strategic position regarding the internet, being the entry point for several major communication cables connecting the United States and the United Kingdom with the European continent.

Unsurprisingly the Dutch media and subsequently the public and politicians reacted to the international media reports on so-called mass surveillance programs by questioning the role of the Dutch intelligence and security

services; do they engage in mass surveillance gathering and how far does their cooperation with foreign services go?

Scope of the investigation

In July last year, the Dutch Parliament requested an investigation by our Committee into the conduct of the Dutch civil and military intelligence and security services. The request included a number of questions to be answered by our Committee. We complied with the Parliamentary request and embarked on investigation number 38. The processing of telecommunications data by the Dutch services was the focal point of this investigation. We discussed three different aspects of data processing in our report, namely the acquisition of data, the storage and use of data and the exchange of data with foreign services.

In line with the Parliamentary request, investigation no. 38 focussed on the following topics:

1. The scope of the general and special powers of the services to process telecommunications data and how these powers relate to the Constitution and human rights law (the ECHR);
2. The way in which the services use the different types of data files and the rules applying to such use;
3. The way in which the human rights safeguards play a role in data processing by the services, in particular in the exchange of data with foreign services.

Due to the urgency of the matter and the broad scope of the necessary investigation, our Committee decided to concentrate on the procedures of the services instead of individual operations. In-depth analysis of operations in relation to this topic is to be covered mainly by our Committee's investigation

into the activities of our General Intelligence and Security Service (GISS) on social media, expected to be published at the end of August.

Conclusions

The main conclusion of our Committee's investigation was that, in general, the procedures used by the Dutch services fall within the scope of the powers conferred on them by law. There is no question of them systematically processing collections of personal data in disregard of the law.

Specifically, our Committee established that:

1) The services do not practice untargeted mass interception of cablebound communication – this is communication via cables such as internet traffic - which means that they comply with our law which does not allow for this type of interception.
2) There was no indication that the Dutch services had sidestepped legal restrictions by requesting foreign services to collect data by a method they are not themselves permitted to use.

However, this picture of legality is not the whole story. First of all our Committee found certain practices involving the deployment of human sources – namely agents or informers - in this field to be unlawful. Secondly, there is an unlawful practice in the field of sigint. Lastly, there was a case of unlawful conduct where the military service didn't comply with the legal requirements in providing support to foreign services.

But perhaps the most important conclusion, especially for the future, is that data processing has radically changed since the Dutch Intelligence and Security Services Act was adopted in 2002. Technological developments - and consequently the digitalisation of society - have not only largely facilitated

digital communication and the digital storage of large volumes of data by individuals, they have by that consequently also increased the possibilities of the services to acquire, process and exchange this data. This means that there is much more personal data available for processing than ever before. These developments have led to a greater potential for privacy infringement by the services than was foreseen in 2002. Because this potential privacy infringement has not yet been adequately addressed by the Dutch law, our Committee sees this as a gap between the activities of the services and the safeguards which are necessary to regulate these activities.

We realise that this problem is by nature not a purely national affair; it is intrinsic to the digitalisation of society on a global scale.

Examples of specific findings of our Committee that relate to this issue and that call for an amendment of our Intelligence and Security Services Act are the following:

1) There is no separate legal regime for metadata analysis under current Dutch law, while this method is nowadays widely and increasingly used by the services for a number of purposes such as social network analysis.
2) Our current law sets no time limits for the storing of unprocessed data. This is unsatisfactory because unprocessed data usually includes the data of persons who do not form a threat to national security. This data should not be subject to unlimited storage for the sole purpose of possible use in the future. In general, our Committee observes that the more data the services collect, the greater the urgency to discard the data that is irrelevant to the national security at that time.

On the subject of international cooperation our Committee called attention to the fact that in some cases, the use of data received from foreign partners can

come into conflict with human rights obligations, such as the obligation to guarantee the right to privacy. In the light of the recent allegations our Committee holds the opinion that the current situation, in which close cooperation relationships are largely based on trust that foreign partners respect human rights and act within their own legal boundaries, no longer does justice to this concern. First of all, such trust needs to be based on sufficient knowledge of the competences and possibilities of foreign partners. Besides this, our report includes the recommendation that our ministers take steps to improve transparency in cooperation relationships and that they specify the conditions which must be satisfied in order for the cooperation to be lawful.

Follow-up

Our report was presented to Parliament last March. Both the minister of the Interior and the minister of Defence indicated in their letters to Parliament that they would comply with all the recommendations of our Committee. Among other things, this means that the ministers will be taking steps towards greater transparency in international cooperation between services. The Parliamentary debate following the presentation of the report led, among other things, to the acceptance of a proposal by Parliament regarding further implementation of the criteria for cooperation with foreign services.
Recently, the minister of the Interior reported that the Dutch services are taking part in an initiative to develop common standards on international cooperation between EU member states. This initiative is part of the so-called Eight-Point Program for Privacy Protection the German Chancellor Mrs Merkel presented at her annual Summer press conference in July 2013.

Concluding remarks

I would like to call your attention to an issue which lies at the core of international cooperation between services. In our report we included an appeal to the wider intelligence community for more transparency between services that work closely together. Though we are aware of the fact that there are many obstacles on the road to greater transparency in the field of secret services, our Committee strongly feels that now is the time to take definite steps in that direction due to the international momentum. I would like to underline that this goal of greater transparency can only be reached if all our services are prepared to offer their international partners a certain level of insight into their methods and sources.

For its part, our Committee contributes to this transparency by publishing English translations of many of its reports. These reports provide insight into the competences and practices of the Dutch services and into their compliance with both the Dutch law and human rights law. In this way a body of international jurisprudence can be built on this important topic.

As a newcomer in the field of oversight, I will be delighted to hear your experiences and opinions. In particular I am curious to hear the possibilities you see for increased transparency.