Remarks of Ian Leigh, Professor of Law, Durham University[1]

Workshop 2: Fostering cooperation and exchange of best practices between intelligence oversight bodies in the EU

Dear Chairman, Ladies and Gentlemen it is a pleasure to be able to participate in this important event and I grateful for the invitation and for the support of the Belgian Parliament in making it possible for me to attend.

I will focus my remarks on the barriers to intelligence oversight cooperation and on possible solutions to them.

I shall argue that the main barriers to intelligence oversight cooperation relate to the mandates of national oversight bodies, limitations on access to information concerning intelligence cooperation, and the third party rule.

Mandate

Very few statutes regulating external oversight of intelligence explicitly mandate scrutiny of international intelligence cooperation.[2] Revelations about the human rights implications of international intelligence cooperation in the context of counterterrorism have compelled some oversight bodies to examine aspects of international intelligence cooperation but this is a relatively recent development. In most countries, however, international intelligence cooperation remains an under-scrutinised area of services' work; many oversight bodies have yet to examine in a systematic or regular manner their services' cooperation with foreign partners. Various factors may explain this including the mandates of oversight bodies, sensitivities surrounding international intelligence cooperation, difficulties in acquiring necessary information, competing priorities and a lack of resources.

Even where legislation does clearly apply to cooperation it only mandates standing oversight bodies to monitor intelligence

[1] This presentation draws on a work that forms part of a forthcoming policy handbook co-authored with Aidan Wills and Dr Hans Born on oversight and international intelligence cooperation, to be published by DCAF-EOS in October 2015.

[2] Rare exceptions include Canada's CSIS Act, which requires the services to provide the SIRC with copies of cooperation agreements/MoU.

services in their own state. They are responsible for evaluating their country's intelligence services' actions regarding, for example, information sharing, joint operations and handling requests received from foreign partners. Overseers conduct such assessments and hold their country's officials to account in accordance with national law. It is not their role to scrutinise the actions or policies of foreign services and their governments. For example: overseers might examine whether a decision by their service to send information to a foreign partner was taken in accordance with policy and the law. They could not, however, carry out a corresponding assessment of a request submitted by a foreign service. They have neither the legal mandate nor the powers to scrutinise and pass judgment on the actions of foreign entities

There are nonetheless a number of aspects of international intelligence cooperation that overseers may wish to scrutinise on the basis of domestic law, policy and operations of their own services. These include:

The Effectiveness of cooperation with foreign entities

- Legal and (operational) policy framework for international intelligence cooperation
- High-risk relationships and Risk assessment processes
- Personal data exchanges and the use of Caveats and assurances relating to information sent to foreign services
- Reporting and records keeping
- Joint operations
- Provision of training and equipment to foreign services
- Services' training of their own staff
- Financial transactions relating to international intelligence cooperation
- Role of the executive in international intelligence cooperation

These are topics which are covered in some depth in a forthcoming policy guide that I will describe at the end of my remarks but which time does not permit me to go into in depth.

Access to information

A number of states limit overseers' access to information on international intelligence cooperation. Firstly, laws regulating

oversight bodies sometimes explicitly prevent an oversight body from viewing information provided by a foreign entity. This is the case in, for example, with regards to parliamentary oversight committees in France and the UK. Second, and more commonly, laws include general restrictions on access to operational information by oversight bodies (and information about international intelligence cooperation is deemed to fall within this). Finally, some national laws contain provisions granting the executive broad discretion to determine what information can be provided to an oversight committee. This may be exercised in order to bar an oversight body from examining information relating to international intelligence cooperation.

Statutory limitations do not necessarily undermine oversight as long as there is another external oversight body that has full access to such information and provided that they do not preclude the oversight body from fulfilling its legal mandate. In both Australia and South Africa, for example, a non-parliamentary expert body (an inspector general) has full access to all relevant information denied to parliamentarians. Where there are no such compensating arrangements, however, there is a risk of a blind spot in oversight.

Third party rule

The *third party rule* is intended to ensure that services retain some control over information sent to foreign partners, including preventing it from being transmitted to a third party that may use it in contravention of human rights. However, the rule can also serve to constrain oversight- especially if services and/or their partners view oversight bodies as third parties. This would imply that a service would need to seek the permission of a foreign partner before its own oversight body could view information provided by that partner.

Such a process of seeking and granting such permission has the potential to seriously undermine oversight. It grants foreign services an effective veto on the scope of intelligence oversight in another state. It is also open to abuse. Services could (mis)use the third party rule to shield certain activities or files from external scrutiny by implicitly encouraging refusal of access when supposedly ‘seeking’ the requisite permission from a foreign

partner.

Moreover, because they are aware the sensitivities of cooperation, some overseers will refrain from requesting their services to submit requests to a foreign partner in the first place. On the other hand the idea that a partner state may consent to publication in an overseers report of information derived from it should not be dismissed as fanciful- the *2014 Report of the UK Intelligence and Security Committee into the intelligence surrounding the murder of Fusilier Lee Rigby* is a recent example of consent being sought and given for publication, even in a country where the services have stubbornly championed the third party rule.

An increasing number of oversight bodies, however, refuse to accept that they are third parties or that their services need to obtain the permission of foreign partners before their overseers can view information. The 2015 report of the Venice Commission endorses this approach. Institutions such as the SIRC, CTIVD and EOS Committee have taken the position that statutory provisions granting them access to all relevant information held by services override any limitations that may arise from the third party rule. (Of course, such a practice does not allow the oversight bodies to further disseminate the information concerned without permission.)

Bearing all this in mind, when drafting statutory provisions on oversight, legislators may need to be more explicit about the right of overseers to access information regardless of its provenance.

There are particular barriers to oversight in relation to personal data sharing and use of caveats that deserve mention in the light of recent controversies.

Personal data exchanges and cooperation

There is a strong case for external oversight of the policies and processes for exchanging data with foreign entities, as well as specific instances of personal data sharing. Given the volume of personal data that is shared and limited resources available to overseers, they may, however, consider focusing on personal data sharing policies and processes. In the UK, for example, the Intelligence and Security Committee in its report on *Privacy and*

Security: a modern and transparent legal framework has argued that a clearer statutory basis is needed.

Oversight of personal data exchanges with foreign entities in specific cases is most likely to be a task for expert non-parliamentary oversight bodies and/or privacy and information commissioners. This is because it demands a depth of scrutiny that parliamentary committees do not normally have the time, expertise or resources to conduct.

Such overseers can scrutinise factors such as whether the data exchange: complied with applicable laws; was properly recorded; whether appropriate caveats were attached to the information; and/or any assurances were sought from a foreign service. If personal data is transferred on the basis of a request from a foreign partner, overseers can examine whether it was reasonable to send the information in view of the scope and preciseness of the request.

By way of example, this has been a focus of Norwegian EOS Committee's oversight of international intelligence cooperation. The Committee regularly examines personal data exchanges to assess who data was sent to, whether disclosures were made for lawful purposes and whether they are proportionate from a human rights perspective.

Potential Solutions

I have mentioned several obstacles to oversight arising from intelligence cooperation. The question arises as to whether oversight bodies could cooperate to overcome these challenges?

It could possibly be argued that, since intelligence services can transmit classified information to foreign counterparts, overseers should be permitted to do the same. There may be situations in which information from foreign overseers could assist a domestic investigation- for example with regard to the use made by a partner agency of outgoing information or the actions of a partner agency in a joint surveillance operation conducted on home soil. In each case this could help the oversight body to understand its own service's role.

Although direct information exchange of this kind between oversight bodies might appear logically appealing there are substantial difficulties.

Information (about and from intelligence services) accessed by oversight bodies does not become *their* information and they are not usually free to share it with foreign oversight bodies. In most instances intelligence services are unlikely to agree to a request from their overseers to transmit classified information to a foreign oversight body. More likely they would resist, not least because they have no relationship with these bodies and may be unsure whether to trust them with information.

Mutual oversight assistance

It might be more realistic for oversight bodies to cooperate through mutual requests to examine particular issues and the sharing of unclassified conclusions.[3] Two or more oversight bodies could devise a mechanism whereby they can request (or recommend) their counterpart(s) to examine a particular aspect of international intelligence cooperation from 'their' side of their relationship- for example whether outgoing information has been used in accordance with caveats imposed, or whether incoming information was collected in compliance with the law. Alternatively, where one country's service asserts to its oversight body that a foreign intelligence partner has vetoed disclosure of information that it supplied, the oversight body could request its counterpart to check that such a request was indeed made and refused. In neither instance would there be any need for classified information to cross borders from one oversight body to another.

A similar process could also be used by an oversight body to raise concerns with counterpart, so triggering additional scrutiny in the partner country.

Admittedly for such cooperation to function, oversight bodies and their services would need to have close relations and the oversight bodies would need to have comparable mandates. Where these conditions apply, however, mutual oversight assistance could help

[3] Craig Forcese,'The collateral casualties of collaboration: the consequences for civil and human rights of transnational intelligence sharing,' in *International Intelligence Cooperation and Accountability*, 89-91; and Aidan Wills and Hans Born, 'International Intelligence Cooperation and Accountability: Formidable challenges and imperfect solutions, in *International Intelligence Cooperation and Accountability*, 301-302.

to promote better oversight on both sides of an intelligence cooperation relationship.

Towards European Standards?

Finally concerning the question of the feasibility of European standards for intelligence oversight, I would like to briefly mention a report that, together with colleagues from DCAF and EOS, I am in the final stages of producing. The process of developing it has been a multi-year project of studying legislation and reports from a number of countries, as well as relevant court cases and international standards. It has involved interviewing a number of former senior intelligence officials of different countries and current overseers. The draft report has been critically scrutinised by an international advisory board comprising such practitioners.

The report will cover the benefits of intelligence cooperation, as well assume of risks that have recently been highlighted. It will stress the need for oversight and accountability, not only through internal controls, but also external to agencies- in the executive branch, through parliamentary and expert oversight bodies- and examine the place of review by courts, both domestically and internationally.

The ambition is not to create a super-national structure nor an international code (of even the loosest kind, such as the Codex proposed by the PACE Rapporteur). Rather, it intended an as analysis of emerging best practice that can be used as a resource especially by national parliamentarians, executive bodies and overseers. Many countries are grappling with common questions in this field- as this conference has shown. Although oversight bodies in some are at a very early stage, there is much that can be learned from oversight bodies in countries that are further down the road.

It is intended to launch the report in Oslo in October.

Thank you for your attention. I would be pleased to answer any questions.