BELGIAN SENATE

6th Conference of the Parliamentary Committees for the Oversight of Intelligence and Security Services of the European Union Member States

Brussels, September 30th – October 1st 2010

Friday, October 1st 2010

Prof Dr Iain Cameron (S),
Juridiska institutionen, University of Uppsala

Particular accountability problems relating to International Co-operation between Intelligence Agencies

1. Treaties on mutual assistance between police, customs and judicial authorities are nowadays an important feature of the fight against transnational organised crime. Similarly, as already mentioned, improved international intelligence cooperation is necessary to combat terrorism in particular. However, this necessary improved cooperation can cause problems as far as concerns accountability for security services. Accountability arrangements tend to track the policies or actions of national security and intelligence agencies. Frequently, the legislation contains either express or implied limitations that inhibit oversight or review of arrangements made with the intelligence agencies of other countries.

2. The detention and interrogation of "enemy combatants" in Afghanistan and at Guantanamo Bay, extraordinary renditions, alleged secret detention centres, torture or the use of information obtained by torture in third countries have led to a growing number of inquiries and reports by national and international bodies.[1] Where foreign agencies operate without permission in another State, then this

---

[1] See, e.g. Venice Commission, Opinion on the International legal obligations of Council of Europe member States in respect of secret detention facilities and inter-State transport of Prisoners, CDL-AD(2006)009; Bericht der Bundesregierung (Offene Fassung) gemäß Anforderung des Parlamentarischen Kontrollgremiums vom 25. Januar 2006 zu den Vorgängen im Zusammenhang mit dem Irakkrieg und der Bekämpfung des Internationalen Terrorismus, at http://www.bundesregierung.de/Anlage965868/Bericht+der+Bundesregierung+-+offene+Fassung.pdf.; Parliamentary Assembly of the Council of Europe, Alleged secret detentions and unlawful inter-State transfers of detainees involving Council of Europe member States, report of the Committee on Legal Affairs and Human Rights, 12 June 2006, Doc. 10957; European Parliament resolution on the alleged use of European Countries by the CIA for the transportation and illegal detention of prisoners (2006/2200(INI)).

will be in violation of the national sovereignty of this State, and depending on national law, may give rise to criminal responsibility. Leaving aside this extreme case, it is becoming clear that even collaboration between agencies in different States can give rise to serious concern. National systems of oversight or accountability were designed for a different era and to guard against different dangers of abuse (for instance, interference in domestic politics or civil society by the agencies). They do not address this concern.

3. Concrete examples of abuses involving international exchanges of intelligence are unlikely to come to light, although the recent Maher Arar case is in Canada is an exception.[2] The main obstacles that national accountability bodies face in this task are a combination of "plausible deniability" and lack of powers to supervise such arrangements. Where a security agency merely receives "anonymized" intelligence from an overseas agency with which it has an arrangement, it can argue that it is not responsible for how the information was obtained. A security agency might accept responsibility in theory where it had actively requesting a foreign agency to obtain information from a suspect by means which are not lawful in the receiving agency's State. The problem will be that this level of involvement can rarely, if ever, be substantiated. The receiving agency will almost invariably be able to argue that it had no knowledge of that illegitimate measures have been used to obtain the intelligence, and no reason to suspect that such measures were used. Allegations of illegal or unethical behaviour can be "plausibly denied" since the receiving agency was not responsible for them. A truthful but incomplete denial can therefore be given to any suggestion that the information was improperly obtained by the receiving agency.

4. Moreover, there can be strong incentives for the receiving agency not to inquire into how information was obtained. An agency in a country with limited foreign intelligence gathering capability may be dependent on friendly foreign agencies providing it with intelligence. If the receiving agency asks too many questions, it may well receive embarrassing answers, namely that the material was indeed obtained by unethical means. One could argue that the receiving agency should try to insist that the supplying agency certifies compliance with human rights standards, but the supplying agency may simply refuse.

5. The exercise of police power is primarily national. That means that whatever national restrictions which apply to obtaining information tend only to apply to actions within the territory or to direct actions by State officials. This leaves the clear possibility that an agency may benefit from intelligence collected overseas by another country's agency through means that it would not be legally permitted to use.

6. In so far as one agency supplies information to another country's agency, again accountability is flawed since the information is unlikely to result in a decision that can be directly traced to the supplying agency. Information may be supplied on terms that the source is not revealed to any other body, including the courts or whatever the oversight bodies exist in the receiving State. Even where this is not so the confidentiality of the source of the information may be protected either under legislation in the receiving country or through the actions of its courts in the name of not harming international relations. Where the legal systems of both the supplying and receiving agencies protect the secrecy of international relations in this way, the result is a vacuum of accountability. The supply of information to multi-lateral bodies- for example to the UN Sanctions Committee or, for

---

[2] The Commission of Inquiry into the actions of Canadian Officials in Relation to Maher Arar, Report of the Events Relating to Maher Arar, 3 volumes, 2006, http://www.ararcommission.ca/.

EU States, under the EU Third Pillar bodies may also suffer from comparable defects of accountability.

7. The case-law of the ECtHR is still developing in the area of the extent to which a State can, and should, bear responsibility for acts with an extraterritorial dimension. It is, however, already evident that a vacuum of accountability is not acceptable.[3]

Oversight and International Co-operation

8. As previously explained, there can be a vacuum of accountability as regards international cooperation in security matters. Legislators may be able to aid accountability by creating a legal framework in which co-operation with foreign agencies is only permissible according to principles established by law and where authorised or supervised by applicable parliamentary, or expert control bodies.

9. As the Secretary General has pointed out in his report, this is an area where there are relatively few known examples of rules, agreements or best practices. The Venice Commission will therefore rather try to identify abstract models allowing an adequate oversight of international co-operation.

10. As regards a foreign agency's exercise of public power (e.g. use of special investigative means, arrest, detention, interrogation) in another State's territory, it is vital that this, if it is to be allowed at all, only occurs in accordance with applicable constitutional rules on transfer of authority.

11. Limited transfers of public power are a feature of a number of modern treaties on police and customs cooperation.[4] However, it is vital that the procedure to make a grant of permission to foreign security agencies to exercise police, or security, powers is set out in the constitution, or at least in statute. Decisions to grant authority in a specific case should normally be made only by the competent authority of the State, which will usually be the government, or a government minister, and properly registered.

12. Accountability structures must be in place to ensure that a foreign security agency is not granted permission to exercise security or police functions in another State by junior or middle-ranking officials of that other State. Administrative, and where applicable, criminal responsibility should apply to unauthorised attempts to transfer police or security powers, or passivity when an official knew, or should have known about a foreign agency's unauthorised exercise of police or security powers in the territory of the State. The Secretary-General's report recommends that parliamentary bodies oversee all such decisions to transfer police or security powers. The Venice Commission considers that, although there may, exceptionally, be grounds for not notifying the parliament in advance of a transfer of authority to exercise police or security powers in a specific

---

[3] See, in particular, ECtHR, *Öcalan v. Turkey* judgment of 14 December 2000; *Bankovic and Others v. Belgium* and 16 other Contracting States decision of 12 December 2001; *Assanidze v. Georgia* judgment of 8 April 2004; *Issa and Others v. Turkey* judgment of 16 November 2004; *Ilascu v. Moldova and the Russian Federation* judgment of 8 July 2004. See also below Section V.

[4] See, e.g., Article 41 of the Convention applying the Schengen Agreement of 14 June 1985 between the governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, 1990, 30 I.L.M. 84 (1991).

case, there must afterwards be full governmental accountability to the parliament for all such decisions. [5]

13. As regards the question of transfer of data, this should be regulated in statutory or other rules to avoid a vacuum of responsibility. Both the supply and receipt of data must be regulated by agreements in writing made by the proper authorities.[6] These should be submitted to parliamentary or expert oversight bodies.[7] Conditions should be attached to intelligence transferred. Limits must be placed both on the type of intelligence which can be transferred[8] and requirements must exist to check the reliability and accuracy of the intelligence, before it is transferred and also, for a receiving agency, to check reliability and accuracy when information is received from another State.[9] An example of a supply rule can be found in the German statute governing the BundesVerfassungsschutz, namely "The Agency may provide foreign security and other appropriate foreign services, as well as supra and international organisations, with data regarding citizens, provided that the supplying of this data is essential for the pursuit of its duties or because prevailing security interests of the receiving institution necessitate this. The supplying of information ceases when this would run counter to the predominant foreign concerns of the Federal Republic of Germany or where the pre-eminent interests of the affected private persons deserve to be protected. The supplying of data ought to be recorded in public files. The beneficiary is to be instructed that the information is transmitted on the understanding that the data may only be used for the specific purpose for which it was sent. The Agency reserves the right to request information on the usage of data by the beneficiary."[10]

14. Another, more far-reaching method is to require that information should only be disclosed to foreign security and intelligence agencies or to a supranational body if they undertake to hold and use it subject to the same controls that apply in domestic law to the agency which is disclosing it (in addition to the laws that apply to the agency receiving it).[11] As regards receipt of information, then

---

5 See, e.g., the Law on the Intelligence and Security Agency of Bosnia and Herzegovina, 2004, Articles 70 and 71, Secretary-General's report.

6 See, e.g. the Dutch Intelligence and Security Services Act 2002 (De Wet op de inlichtingen- en veiligheidsdiensten) Article 36(1)(d), 40(1) and 42.

7 See e.g. Canadian CSIS Act, Section 17(2) which requires that the oversight body, the Security Intelligence Review Committee (SIRC) be given copies of all CSIS agreements with foreign governments and international organizations.

8 See, e.g. Article 9 (conditions and limits on supply of data) of the Agreement on Co-operation Between the Republic of Bulgaria and the European Police Office http://www.europol.europa.eu/legal/agreements/-Agreements/15977.pdf which specifies inter alia that "Personal data revealing racial origin, political opinions or religious or other beliefs, or concerning health and sexual life as referred to in Article 6 of the Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data shall only be supplied in absolutely necessary cases and in addition to other information."

9 See Article 10 of the Europol-Bulgaria Agreement, ibid. (assessment of the source and of the information). See also Arar Commission, Report of the Events Relating to Mahar Arar, Analysis and Recommendations, op. cit, p. 334.

10 Bundesverfassungsschutzgesetz (BVErfSchG), Germany, 2002, Art. 19 (Unofficial translation).

11 See e.g. Law on the Intelligence and Security Agency of Bosnia and Herzegovina, 2004, Article 65. A similar purpose could obviously be achieved if common standards could be agreed upon, assuming that these are not the "lowest common denominator".

it should be held subject both to the controls applicable in the country of origin and those standards which apply under domestic law.[12]

15. Foreign-source data should in principle not be excluded from the supervision of whatever data monitoring arrangements exist for data of national origin. However, it may be that especially stringent security arrangements may be permissible for access to such data.[13] The complicating factor is that, as already mentioned, assessing the reliability of intelligence often involves looking at the "raw" intelligence material, not simply the "refined" product. The same applies to assessing the lawfulness of the methods for obtaining the information (ill-treatment during interrogation etc). A foreign agency may be prepared to transfer the product, e.g. that it considers a particular person to be linked to terrorism, or that an attack on a given target imminent, but not the basis for this product.

16. The situation is likely to arise increasingly that a supervisory authority or oversight body in one State is denied access to important foreign-source data which forms part of the reasons behind the general policies or specific operations of its own security agency and which it accordingly considers that there is a pressing need to examine.

17. Where a supplying agency refuses to accept that the information supplied is subject to the standards and supervision applicable in the receiving State, there are a number of options. The first is that the receiving agency is required to refuse to accept information which the sending agency would refuse to permit the supervisory body to examine, if it chooses to do so. This option will be very unpopular with the receiving agency, especially if it is in practice partially dependent on foreign-source data to do its job of securing the security of its State and individuals in it.

18. The second option is that the supervisory authority or oversight body in the receiving State accepts that it has no access to the raw material or even the refined product transferred, but that it instead accepts a certification issued by whatever equivalent independent supervisory authority or oversight body exists in the sending State that the data is reliable according to the standards applied in the sending State, and that it was lawfully obtained.

19. This option will not exist inter alia where transferring data to, or receiving data from, a State with a suspect human rights record, as there will be no independent supervisory body in the transferring State. In such cases, where the agency nonetheless feels that security considerations require such transfer/receipt of data, it should be a requirement on the agency to take into account the human rights implications of this transfer/receipt before it takes place, and to mitigate whatever

---

[12] See Born H. and Leigh, I. *Making Intelligence Accountable: Legal Standards and Best Practice*, chapter 12.

[13] The European Commission on Human Rights accepted in Volpi v. Switzerland (No. 25147/94, 84 DR 106 (1996)) as regards transfer of data that particularly stringent restrictions can apply to allowing access to foreign-source data. However, it meant that foreign-source data could be excluded from members of the public who had been granted access to their own (no longer active) security files, not excluding access to such information to even the State's data protection bodies.

risks might arise as a result of such cooperation.[14] This latter option is not optimal, but it is a minimum standard which would reconcile security, and human rights concerns.[15]

20. Finally, it should be stressed that the networking which security agencies engage in is a legitimate, and necessary, response to the problems of network threats, such as some modern forms of terrorism. The correct response on the part of national parliamentary oversight and/or expert oversight bodies which exist is also to engage in networking. Parliamentary and expert bodies may be able to overcome hurdles to accountability by sharing information that they acquire about intelligence co-operation, obviously within the limits of the secrecy rules applicable to them. At the very least, they can exchange information on "best practices" in general terms on trends and problems which have emerged in their work and in making available to one another the published evidence from equivalent investigations and reports. A model for such cooperation can be found in the periodic meetings which are held of police oversight bodies in European States.[16]

_____

[14] Arar Commission, Report of the Events Relating to Mahar Arar, Analysis and Recommendations, 2006, p. 348.

[15] It would not, however, solve the problem of transfer of data by supranational bodies, unless and until supranational supervisory bodies are created. Having said this, the supranational bodies which do exist have little or no independent intelligence gathering capacity at the present time, and thus mainly, or exclusively, receive information.

[16] See, for the most recent published conference of Police Monitoring and Inspection Bodies, http://www.igai.pt/publicdocs/Papers_Conference2005.pdf.