EUROPEAN PARLIAMENT 2009 - 2014

Committee on Civil Liberties, Justice and Home Affairs

12.12.2013

WORKING DOCUMENT 5

on Democratic oversight of Member State intelligence services and of EU intelligence bodies

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Claude Moraes

Sophie In't Veld (Co-author)

Cornelia Ernst (Co-author)

The importance and challenges of efficient oversight of intelligence services

- The existence of intelligence services in democratic countries requires strong oversight and accountability mechanisms. Intelligence services are given special, intrusive powers and capabilities in order to protect the state, its citizens and democratic order. However, given the extent of these powers, there exists the potential that they could be used to undermine the security of individuals and subvert the democratic process. Therefore, checks and balances are crucial in ensuring that the intelligence services fulfil their responsibilities in accordance with the constitution and the rule of law.

- In other fields, checks and balances are put in place by rules, controls and democratic/public scrutiny mechanisms aiming at minimising the potential for illegal conduct and abuse of power. However, the high level of secrecy that is intrinsic to the intelligence services - in order to avoid endangering on-going operations, revealing modus operandi or putting at risk the lives of agents - impedes full transparency, public scrutiny and normal democratic or judicial examination.

- The resulting lack of accountability in combination with the special powers that intelligence services enjoy bears a high risk of abuse of power, illegality and a culture of impunity, especially taking into consideration the temptation to use the granted special powers for other purposes than the protection of national security (for instance for economic/industrial or diplomatic espionage or for political reasons). Given these dangers, countries are facing the challenge of creating specific oversight mechanisms to hold intelligence services to account for their policies and actions in terms of legality, propriety, effectiveness and efficiency, while ensuring confidentiality.

- The exact form of oversight varies widely among countries. However, it usually consists of: i) *ex ante* oversight as to the legal framework including mandate and powers of the intelligence services, some form of fundamental rights assessment and prior authorization of certain intelligence operations that infringe on individual rights, and ii) *ex post* oversight by parliamentary or expert bodies, independent of the incumbent government, monitoring the behaviour of the intelligence services and ensuring the respect of the rule of law on behalf of the electorate.

- Most of these national oversight mechanisms and bodies were set up or revamped in the 1990s. However, implementation across Europe has been uneven, with some oversight bodies relatively weak in terms of mandate and powers.[1] This situation has been aggravated by parallel developments: rapid technological developments, changing nature of security threats, and international mobility of data, leading to declined relevance and effectiveness of national oversight mechanisms.

Rapid technological developments

- Modern information and communication technologies enable intelligence services to collect information on a mass scale. The revolutionary development in data storage and analysis capacities (data mining, profiling, etc.) further encourages the collection of increasingly vast quantities of personal data in order to extract relevant information or

[1] See also "Parliamentary oversight of security and intelligences agencies in the EU", study for the European Parliament, 2011.

patterns out of them (connecting the dots).

- These technological developments have enabled a certain shift in the paradigm of intelligence services, away from suspicion based, targeted monitoring towards more generalised massive, and systematic surveillance.

Changing nature of security threats

- The nature of security threats has changed drastically with the technological developments, making them more international, heterogeneous and asymmetric. This has increasingly led to (international) intelligence cooperation, also involving the exchange of personal data, and often blurring the line between intelligence and law enforcement cooperation.

Availability and mobility of data

- Increase in internet bandwidth and the development of mobile computing devices have led to an exponential growth in the amount of personal data available in digital form (email traffic, web searches, internet phone calls, geo-location, financial transactions, medical files, etc). Increasingly, our identity can be distilled from this "digital footprint" of available online personal and meta-data.

- These personal digital data, transiting through cables or satellites and stored/processed within cloud computing services around the world, can rather easily be intercepted/collected by intelligence services.

- As the world becomes more and more wired and interconnected, these data are increasingly stored and transmitted freely across borders and through transit countries, leading to an unclear situation regarding jurisdiction and diminishing the relevance of national legislation and of national oversight.

Challenges to national oversight of intelligence bodies

- The above mentioned trends lead to the following paradox: While legislation and oversight concerning intelligence services is regulated on a national basis, security threats, intelligence information and personal data increasingly transcend national borders. This can result in the flow of information from highly protective environments to less protective jurisdictions, circumventing national legislation. For example, the extraction of certain information by a foreign intelligence service and its return under the head of intelligence sharing to the national intelligence service can be used by the latter to "launder" this information and to circumvent national legislation that safeguards privacy protections it would otherwise enjoy.

- Domestic oversight bodies may have jurisdiction over the sending agency or the receiving one but not both of them, leading to gaps in which information exchanges can take place without adequate review. This problem is further aggravated by the so-called "third party rule" or the principle of "originator control", which has been designed to enable the originator to maintain control on the further dissemination of its sensitive information, but is sometimes also interpreted as applying to the recipient services' oversight. Some intelligence services are reluctant to request the permission of originating services to

transmit intelligence to oversight bodies, while reviewers, conscious of the services' reputational concerns, rarely demand that the services make such requests.

- Given the power of the third party rule to shield swathes of information, the expansion and acceleration of international intelligence cooperation presents thus a formidable challenge to accountability processes. This problem will likely be further increased by technological developments that will increase the amount of communications subject to potential interception by foreign intelligence agencies to the point that, if left unregulated, national laws would become moot.

- While both the threats to national security and the responses to these threats have become increasingly globalised, accountability mechanisms have remained territorially bounded. The growing cooperation between national intelligence agencies has not been adequately matched by international collaboration between national oversight bodies. Ultimately, the combination of the weakness of these bodies on the one hand, and the levels of secrecy, sensitivity and multi-territoriality inherent in international cooperation activities on the other, has led to an increasing accountability deficit and made in certain cases intelligence sharing an area of relative impunity To a certain extent, the lack of transparency surrounding international agreements concerning intelligence agency cooperation has aggravated the problems described above.

- National oversight bodies were designed for a different era, and in response to a very different set of abuses and are hamstrung by inadequate legal powers to access all information and fully hold intelligence services to account. These bodies seem thus to be ill equipped to hold intelligence services and their political masters to account in present days of international cooperation, technological developments and mobility of data.[1]

Solutions

- One avenue is to increase transparency and thus public scrutiny. While full transparency is not possible in this field, intelligence services tend to have an excessive or even obsessive attitude towards secrecy. Confidentiality should be regarded more as an exception, demanding convincing justification motivated with reference to specific and significant harm that might arise from public disclosure of information, instead of being simply based on the broad and ambiguous concept of "national security". Criteria could be developed on enhanced transparency, building on the general principle of access to information and the so-called “Tshwane Principles”.[2] These criteria would need to be binding on the governments in order to have any effect.

- A second avenue is to strengthen national oversight systems. This should be done in terms of *ex-ante* authorization by an independent investigating magistrate who is well-trained in the judicial assessment of human rights. Furthermore, the *ex-post* oversight of their activities by parliamentary or independent expert bodies should be strengthened by providing them with full access to information (including classified information and information from other services), the power to conduct on-site visits, a robust set of

[1] I. Leigh, Accountability and intelligence cooperation.
[2] The Global Principles on National Security and the Right to Information, June 2013.

powers of interrogation, sufficient technical expertise, adequate resources and strict independence from the government. In general, these bodies should also be obliged to report to their respective parliaments. This should be complemented by setting binding minimum European standards or guidelines on the oversight of national intelligence services, building on existing best practices and recommendations by international bodies (UN, Council of Europe, etc).

- A third suggestion is to allow for oversight bodies to keep pace with the activities being overseen. Since intelligence services have to cooperate with each other in order to tackle threats and networks across borders, oversight bodies need to cooperate on an international level as well in order to hold intelligence services accountable. Recognising the need for increased cooperation between national review bodies of intelligence agencies[1], a platform has been established allowing oversight bodies to share common problems and best practices.[2] This call for increased collaboration was further substantiated with the signing of the Declaration of Brussels which recognises the need for more intensive exchange of information between the parliamentary oversight bodies of the EU Member States, Switzerland and Norway.[3] So far, this happened uncoordinated, whereas there is room for more conscious international collaborative oversight. This could take place through joint committees, sharing of information or the creation of supranational bodies. This could be achieved through a body similar to the Article 29 Working Party in the field of data protection.

- A High-Level Group could be set up to propose, in a transparent manner and in collaboration with parliaments, further steps to be taken for increased oversight collaboration in the EU, including the oversight of the EU Intelligence Analysis Centre (IntCen).

- Weak formalised national systems of intelligence accountability could be counterbalanced by more informal accountability through revelations provided by investigative journalists in tandem with activists and whistle-blowers. This requires however not only a better legal protection for them, but also a break on uncontrolled surveillance that can create a chilling effect on these same persons. Also here the "Tshwane principles" as well as the work performed by the Council of Europe could act as an inspiration for further development. It should be noted however, that a proper mechanism for oversight should not be depending on journalists and whistleblowers, and be equipped with powers that enable it to achieve its goals on its own.

- An area of concern in relation to the scope of oversight mechanisms is the evident overlap between the operation of intelligence agencies and the scope of traditional policing. Given that there is a strong framework of accountability and stricter rule of law in the former, it is imperative that oversight mechanisms ensure that fundamental rights are protected within the scope of intelligence activities.

Questions for debate

[1] http://www2.ohchr.org/english/issues/terrorism/rapporteur/docs/A.HRC.10.3.pdf
[2] See for example ENNIR - The European Network of National Intelligence Reviewers (www.ennir.be).
[3] http://www.parlement-eu2010.be/pdf/30sep-1okt-declarationE.pdf

- Given the extent of international cooperation by intelligence agencies in the EU it is crucial that the scope of this activity is subject to adequate control allowing oversight bodies to scrutinise international intelligence cooperation. There is a threat that with international cooperation, intelligence agencies in EU Member States may be able to receive communications that they could not otherwise lawfully gather themselves. As stated, the third party rule can serve as a barrier to proper oversight mechanisms if the established oversight committee is deemed as a third party. How can it be ensured that information received from a foreign or international agency is subject to adequate oversight? Would it be possible that oversight bodies were not considered as third parties?

- How can national security measures, with a disposition towards the use of obscurity/ambiguity, be embedded in a democratic framework of parliamentary and judicial oversight?

- What should the role and powers of the European Parliament be to exercise parliamentary oversight? Should the European Parliament create a specialized (sub-)committee that is able to receive and scrutinize classified information? How could the EP's "power of the purse" (budget right) be used most effectively to support the possible increased role of scrutiny for the EP?

- If more cooperation and exchange of information takes place among national intelligence services, is it still effective to have exclusively national rules and oversight mechanisms for intelligence services within the EU? How to best organize within Europe collaborative oversight of intelligence services?

- Can national oversight mechanisms, given the technological developments and the mobility of data, ensure that the civil rights of all EU citizens are respected by the different national intelligence services? If not, is there a need for minimum European standards or rules that intelligence services should adhere to regarding information exchange, data protection, transparency and oversight?