
**ADVANCE EDITED
VERSION**

Distr.
GENERAL

A/HRC/10/3
4 February 2009

Original: ENGLISH

HUMAN RIGHTS COUNCIL
Tenth session
Agenda item 3

**PROMOTION AND PROTECTION OF ALL HUMAN RIGHTS,
CIVIL, POLITICAL, ECONOMIC, SOCIAL AND CULTURAL
RIGHTS, INCLUDING THE RIGHT TO DEVELOPMENT**

**Report of the Special Rapporteur on the promotion and protection of
human rights and fundamental freedoms while countering terrorism,
Martin Scheinin***

* Late submission.

Summary

Following the introduction, chapter I of the present report highlights the key activities of the Special Rapporteur, from 17 December 2007 to 31 December 2008. The main report, contained in chapter II, highlights several concerns of the Special Rapporteur regarding the role of intelligence agencies in the fight against terrorism. Section A stresses the need for a specific and comprehensive legislative framework to regulate the broader powers that have been given to intelligence agencies in the aftermath of the terrorist attacks of 11 September 2001. The collection and sharing of “signal” intelligence has led to several violations of the right to privacy and the principle of non-discrimination, while “human intelligence” - the gathering of intelligence by means of interpersonal contact - has even led to violations of jus cogens norms such as the prohibition against torture and other inhuman treatment.

Evidence suggests that the lack of oversight and political and legal accountability has facilitated illegal activities by intelligence agencies. This issue is addressed throughout the report, but in section B of chapter II the Special Rapporteur examines in particular the challenges that the increased cooperation between intelligence agencies pose in this context. He clarifies the human rights obligations of States when their intelligence agencies perform joint operations, participate in interrogations and send or receive intelligence for operational use.

When unlawful conduct by intelligence agencies occurs, it may have been condoned or even secretly directed by government officials. In this context the Special Rapporteur looks into best practices of different oversight bodies. In section C he emphasizes that domestic State secrecy or public interest immunity clauses cannot discard their positive obligations under human rights law to conduct independent investigations into severe human rights violations and provide the victims of these violations with an effective remedy.

The concluding section makes recommendations to different key actors (intelligence agencies, domestic legislative assemblies, domestic executive powers and the United Nations) in order to improve the accountability of intelligence agencies in the fight against terrorism.

CONTENTS

	<i>Paragraphs</i>	<i>Page</i>
Introduction	1 - 2	4
I. ACTIVITIES OF THE SPECIAL RAPPORTEUR	3 - 24	4
II. THE ROLE OF INTELLIGENCE AGENCIES AND THEIR OVERSIGHT IN THE FIGHT AGAINST TERRORISM	25 - 63	7
A. Broadening powers granted to intelligence agencies and the need for ex ante accountability mechanisms	26 - 46	7
B. Intelligence cooperation	47 - 57	16
C. Ex post facto accountability and the right to an effective remedy	58 - 63	21
III. CONCLUSIONS AND RECOMMENDATIONS	64 - 78	23
A. Conclusions	64	23
B. Recommendations	65 - 78	24

Introduction

1. This report is submitted to the Human Rights Council by the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, pursuant to General Assembly resolution 62/159 and Human Rights Council resolution 6/28. The main report highlights the activities of the Special Rapporteur from 1 November 2007 to 31 December 2008 and focuses thematically on the role of intelligence agencies and their oversight in the fight against terrorism. The addenda contain a communications report¹ and the report on the fact-finding mission to Spain from 7 to 14 May 2008.²

2. Regarding upcoming country visits, the Special Rapporteur hopes to conduct a mission to Tunisia prior to presenting this report. The Government extended an invitation in June 2008 but has not replied to the request to provide specific dates for the visit. There are outstanding visit requests to Algeria, Egypt, Malaysia, Pakistan and the Philippines. The Special Rapporteur has recently requested visits to Chile, Peru and Thailand.

I. ACTIVITIES OF THE SPECIAL RAPPORTEUR

3. The Special Rapporteur, in accordance with his mandate, undertook a number of activities from 1 December 2007 to 31 December 2008. The highlights are reflected below.

4. From 11 to 14 December 2007 the Special Rapporteur presented his reports to the sixth session of the Human Rights Council in Geneva. He met with the Permanent Missions of Egypt, Israel, Pakistan, Philippines, Russia and the United States of America and participated in two parallel events, namely on “Re-examining international responsibility: inter-State complicity in the context of human rights violations” and “Beyond Guantanamo: protection of human rights while countering terrorism”.

5. From 13 to 14 January 2008 the Special Rapporteur participated in a Joint Arab-European Human Rights Dialogue Working Group Meeting for National Human Rights Institutions on counter-terrorism measures in Cairo. He also met with the Egyptian National Council for Human Rights. On 5 March 2008 he met with the Minister of State for Legal and Parliamentary Councils of Egypt in Geneva to discuss challenges faced by States to ensure the protection of human rights when drafting counter-terrorism legislation.

6. On 13 February 2008 the Special Rapporteur was in Brussels to make a presentation to the European Union Council Working Party on Human Rights (COHOM) and to meet with the European Union Counter-terrorism Coordinator.

7. On 18 February 2008 the Special Rapporteur met with the Permanent Missions of Egypt and El Salvador in Geneva.

¹ A/HRC/10/3/Add.1.

² A/HRC/10/3/Add.2.

8. On 4 March 2008 the Special Rapporteur gave a lecture at the Danish Institute for Human Rights in Copenhagen entitled “Human rights after 9/11 - only a backlash or also an opportunity?”.
9. On 19 March and 28 March 2008, respectively, the Special Rapporteur gave public lectures in Melbourne and Sydney on human rights and counter-terrorism.
10. On 23 April 2008, the Special Rapporteur gave a public lecture on human rights and counter-terrorism in St Petersburg.
11. From 19 to 20 May 2008 the Special Rapporteur participated in the United Nations Counter-Terrorism Implementation Task Force (CTITF) meeting in New York. The Special Rapporteur is a member of the Working Groups on Protecting Human Rights while Countering Terrorism; on Supporting and Highlighting Victims of Terrorism; and on Countering the Use of the Internet for Terrorist Purposes.
12. On 5 June 2008 the Special Rapporteur participated in a teleconference meeting with the Terrorism Prevention Branch of the United Nations Office on Drugs and Crime (UNODC) and made a written submission regarding human rights components which have been adopted in the UNODC draft model on legislative provisions against terrorism.
13. From 9 to 12 June 2008 the Special Rapporteur was in Washington, DC, and gave an informal Congressional briefing organized by the Center on Global Counterterrorism Cooperation. He had a working level meeting with the Legal Affairs Office of the State Department of the United States to discuss legal developments regarding cases before the military commissions at Guantanamo Bay and interrogation techniques of terrorist suspects as a follow-up to his mission report.³ The Special Rapporteur also participated in a panel discussion at the American University on the implementation of the United Nations Global Counter-Terrorism Strategy.
14. On 16 June 2008 the Special Rapporteur was in Prague to participate in the Euro-Mediterranean seminar on ensuring respect for human rights while countering terrorism in accordance with international law, co-organized by the Ministry of Foreign Affairs of the Czech Republic and the European Commission, under the European Union (EU) Presidency of Slovenia.
15. From 23 to 27 June 2008 the Special Rapporteur attended the fifteenth session of the annual meeting of special procedures. He also had high-level meetings with the Permanent Missions of Tunisia and Thailand.
16. On 24 June 2008 the Special Rapporteur chaired an expert meeting in Geneva on “International aviation law: promoting legal safeguards and protecting human rights in the counter-terrorism context”, sponsored by REDRESS and supported by the Office of the

³ A/HRC/6/17/Add.3.

United Nations High Commissioner of Human Rights (OHCHR). Among the participants were legal representatives from the International Civil Aviation Organization (ICAO) and the Venice Commission of the Council of Europe.

17. On 26 June 2008 the Special Rapporteur participated in a panel event, sponsored by the International Council on Human Rights Policy (ICHRP) at the Graduate Institute of International and Development Studies in Geneva, on “Terrorism: risks and choices for human rights organizations”.

18. From 14 to 18 July 2008 the Special Rapporteur conducted consultations in Geneva, in preparation for his reports to the General Assembly and the Human Rights Council. He also met with the Permanent Representative of Pakistan.

19. On 18 and 19 September 2008 the Special Rapporteur convened an expert group meeting at the European University Institute (EUI) in Florence to discuss thematic issues related to his mandate. The meeting was funded by the Åbo Akademi University Institute for Human Rights, through its project to support the mandate of the Special Rapporteur.

20. On 18 October 2008 the Special Rapporteur addressed a workshop in the Norwegian Parliament on “Accountability of international intelligence cooperation”, organized by the Geneva Centre for the Democratic Control of Armed Forces, the Norwegian Parliamentary Intelligence Oversight Committee and the University of Durham Human Rights Centre.

21. From 20 to 22 October 2008, the Special Rapporteur was in New York to present his report (A/63/223) to the Third Committee of the General Assembly. The Special Rapporteur had formal meetings with the Al-Qaida and Taliban Sanctions Committee, the Counter-Terrorism Committee (CTC) and the Counter-Terrorism Executive Directorate (CTED). He met with the Chair of CTITF and with two of its working groups. The Special Rapporteur chaired a follow-up expert meeting on international aviation law which focused on international bodies such as CTC, CTED and ICAO to identify legal tools to help prevent, detect and investigate rendition flights. He also met with a number of non-governmental organizations and gave a press conference.

22. On 27 October 2008 the Special Rapporteur chaired a meeting on the “Principle of legality: defining terrorism and terrorism-related offences”, as part of a regional seminar on upholding human rights while countering terrorism in Amman, organized by OHCHR.

23. On 7 November 2008 the Special Rapporteur participated in an expert seminar on “The impact of terrorism and counter-terrorism measures on the enjoyment of economic, social and cultural rights” organized by the CTITF Working Group on the Protection of Human Rights.

24. From 11 to 12 November 2008 the Special Rapporteur was represented at a stakeholder meeting in New York organized by the CTITF Working Group on Countering the Use of the Internet for Terrorist Purposes.

II. THE ROLE OF INTELLIGENCE AGENCIES AND THEIR OVERSIGHT IN THE FIGHT AGAINST TERRORISM

25. In the course of his mandate the Special Rapporteur has noticed that lack of oversight and political and legal accountability has facilitated illegal activities by intelligence agencies.⁴ Such unlawful conduct may have been condoned or even secretly directed by government officials. This report will therefore reflect upon the human rights implications of conferring broader powers on, and increasing cooperation between, intelligence agencies. It will examine the case law, legislation and practice of a number of Member States in order to clarify the scope of their human rights obligations regarding intelligence agencies and to identify a set of best practices that would improve the accountability and oversight of these services in the context of counter-terrorism operations.⁵

A. Broadening powers granted to intelligence agencies and the need for ex ante accountability mechanisms

26. In general terms the main function of intelligence agencies is to detect potential national security threats, including terrorist threats, by gathering data⁶ and information in such a way as not to alert those targeted, through a range of special investigative techniques such as secret surveillance, interception and monitoring of (electronic) communications, secret searches of premises and objects, and the use of infiltrators. These investigative techniques are effective measures that States may utilize to counter international terrorism.⁷ Their justification can be seen in the positive obligation of States under international human rights law to take preventive measures in order to protect individuals whose life or security is known or suspected to be at risk from the criminal acts of another individual, including terrorists.⁸

⁴ The term “intelligence agencies” is used in this report for agencies with a foreign and/or a domestic mandate.

⁵ The Special Rapporteur is grateful for the assistance of his research assistant at the EUI, Mathias Vermeulen, and for the cooperation of the Geneva Centre for the Democratic Control of Armed Forces (DCAF), the International Commission of Jurists, and the participants of his PhD candidate seminar on legal issues in national, European and international action against terrorism at the European University Institute (EUI), in the preparation of the present report.

⁶ For the purposes of this document the word “data” is used here to describe hard, single, precise facts, which can be used to identify a living person (names, birthday, addresses, telephone numbers, fax numbers, e-mail addresses, vehicle registration data, fingerprints, DNA profiles).

⁷ See for instance: *Klass and Others v. Germany*, European Court of Human Rights (ECHR), 6 September 1978, paras. 48-50, *Murray v. the United Kingdom*, ECHR, 28 October 1994, para. 58.

⁸ The Human Rights Committee has stressed several times that the International Covenant on Civil and Political Rights also protects the right to security of the person outside the context of formal deprivation of liberty. See especially *Delgado Paez v. Colombia*, communication No. 195/1985, Views adopted on 12 July 1990, para. 5.5.

1. A legislative framework for special investigative techniques

27. A crucial first element in ensuring that States and their intelligence agencies are accountable for their actions is the establishment of a specific⁹ and comprehensive legislative framework that defines the mandate of any intelligence agency and clarifies its special powers. Without such a framework States are likely not to meet their obligation under human rights treaties to respect and ensure the effective enjoyment of human rights.¹⁰ An example of best practice lies in the very detailed provisions governing each investigative technique that Dutch intelligence may use.¹¹

28. The approaches of States as to what measures and techniques require judicial approval tend to vary, depending on the scope and strength of the constitutional rights recognized in the State in question, in particular the scope of privacy rights.¹² The mere act of opening a thematic, organization-specific or individual intelligence file may not be seen as raising a human rights issue when there are suspicions that someone is planning to commit a terrorist offence.¹³

29. In this regard, the Special Rapporteur stresses however that information gathered for “strategic intelligence” (i.e. information obtained by intelligence agencies for the purposes of policymaking) must not be used in court proceedings when there is no judicial supervision attached to measures directed at named individuals. The Special Rapporteur has noted with concern that in different courts, the line between such strategic intelligence and probative evidence has become blurred to the advantage of different forms of “national security imperatives”. Judicial approval for a special investigative technique must be given in order to make permissible the use of the fruits of the technique as evidence in court.

30. States may make use of certain preventive measures like covert surveillance or the interception and monitoring of communications, provided that these are case-specific interferences, on the basis of a warrant issued by a judge on showing of probable cause or reasonable grounds; there must be some factual basis, related to the behaviour of an individual which justifies the suspicion that he may be engaged in preparing a terrorist attack. This preventive, intelligence-led approach seeks to anticipate rather than to circumvent legal proceedings and can be a desirable, reasonable and proportionate method to identify risks or to find out more about suspicions against a terrorist suspect. However, States need to be aware that

⁹ See for instance *Kruslin v. France*, ECHR, 24 April 1990, para. 33.

¹⁰ See analogously, *Rotaru v. Romania*, ECHR judgement, 4 May 2000.

¹¹ Intelligence and Security Services Act 2002, arts. 17-34.

¹² European Commission for Democracy through Law (Venice Commission), report on the democratic oversight of the security services, CDL-AD(2007)016, para. 199.

¹³ See for background: *Leander v. Sweden*, ECHR, 26 March 1987, paras. 52-57.

the first sentence of article 14.1 of the International Covenant on Civil and Political Rights is applicable in any matter dealt with by the judiciary and requires compliance with the basic principles of fair trial.¹⁴

31. Although no general norm exists in international law expressly prohibiting or limiting acts of intelligence gathering, it is crucial that States clarify “threshold criteria” that might trigger a whole range of human rights intrusive actions by an intelligence agency, which can range from data mining to covert action.¹⁵ Clear legislated powers for intelligence agencies also help to distinguish between the tasks of intelligence and law enforcement agencies. Failure to make these clear distinctions will lead to blurred lines of accountability and to the risk that special powers are used in routine situations where there is no pre-eminent threat to the population.¹⁶

2. Minimum thresholds for the gathering of information: the problem of data mining and sharing

32. The increasing use of “data mining” by intelligence agencies, entailing the matching of various databases according to a number of variables, blurs the boundary between permissible targeted surveillance and problematic mass surveillance which potentially amounts to arbitrary or unlawful interference with privacy. There is namely an inherent risk of “over-inclusiveness” (meaning that information is gathered because it may be useful, rather than for a defined purpose) in data mining, as the technical capabilities of this technique can tempt the user towards broadening the definition of what is considered suspicious.

33. In this regard the Special Rapporteur reiterates his recommendations on the issue of racial/ethnic profiling.¹⁷ While data mining is not prohibited as such, it should not be allowed to include variables that result in compromising the right to non-discrimination. Data-mining software that performs “sentiment analysis”, which extracts and summarizes opinions from unstructured human-authored documents on the Internet in order to create a terrorist profile - and which is apparently used by intelligence agencies in the United States, Canada, China, Germany, Israel, Singapore and Taiwan¹⁸ - must not be used as the basis for deprivation of liberty or inclusion on “watch lists” that may impede air travel, banking, and employment opportunities at airports or in places where radioactive materials are used, such as hospitals.

¹⁴ See Human Rights Committee, general comment No. 32 (2007) on the right to equality before courts and tribunals and to a fair trial, paras. 7 and 8.

¹⁵ Covert action refers to unacknowledged intervention or measures taken by an intelligence agency in the territory or affairs of another country.

¹⁶ H. Born and I. Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Activities* (Oslo, Publishing House of the Parliament of Norway, 2005), p. 29.

¹⁷ See also, in general, the Special Rapporteur’s remarks on the use of counter-terrorism practices that are based on terrorist profiles that include characteristics such as the presumed “race”, ethnicity, national origin or religion of a person (A/HRC/4/26, para. 59).

¹⁸ The Economist, 25 September 2008.

34. In combination with the frequent problem of poor-quality data, which can be wrongly recorded, wrongly interpreted or outdated when matched with other databases,¹⁹ major concerns arise that innocent people are identified as terrorist threats.²⁰ These potential flaws in data collection are a cause of concern for the Special Rapporteur, especially as there is an increasing trend of facilitating personal data sharing amongst intelligence and law enforcement agencies at the national level and across borders within bilateral or multilateral frameworks such as the North Atlantic Treaty Organization (NATO) or the Shanghai Cooperation Organisation.

35. As a general element of best practice the Special Rapporteur invites Member States to adopt legislation which embodies basic data protection principles reflected in documents such as the guidelines concerning computerized personal data files adopted by the General Assembly in resolution 45/95.²¹ These guidelines start with the principle that “information about persons should not be collected or processed in unfair or unlawful ways, nor should it be used for ends contrary to the purposes and principles of the Charter of the United Nations”.²² This includes the obligation of all Member States to promote and respect human rights. The Special Rapporteur emphasizes that any departures from the principles of accuracy (art. 2), purpose limitation (art. 3), or access (art. 4) should be narrowly constructed. The Special Rapporteur reminds States especially of the fifth principle (non-discrimination, art. 5) that data “likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union, should not be compiled”, and therefore should not be shared either. Exceptions to the fifth principle may be authorized only within the limits prescribed by the International Bill of Human Rights and other relevant instruments in the field of protection of human rights and the prevention of discrimination. In this context, the Special Rapporteur has serious concerns about the sharing of data and information between intelligence agencies in China, Russia, Kazakhstan, the Kyrgyz Republic, Tajikistan and Uzbekistan within the framework of the Shanghai Convention on Combating Terrorism, Separatism and Extremism. This sharing of data and information is not subject to any meaningful form of oversight and there are no human rights safeguards attached to data and information sharing.

36. The Special Rapporteur refers to best practice where the supply and receipt of data between intelligence agencies and its subsequent use is regulated by written agreements made

¹⁹ See F. Bignami, “Towards a right to privacy in transnational intelligence networks”, *Michigan Journal of International Law*, vol. 28, No. 3 (2007), p. 668.

²⁰ See for instance the case of Bisher Al-Rahwi, documented in Amnesty International, *State of Denial: Europe’s Role in Rendition and Secret Detention* (London, Amnesty International Publications, 2008), p. 11.

²¹ See also, on a regional level, European Commission Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Working Document: Transfers of personal data to third countries: applying articles 25 and 26 of the EU data protection directive, 24 July 1998.

²² E/CN.4/1990/72.

between the proper authorities.²³ As an element of best practice, these agreements can be submitted to oversight bodies,²⁴ which ideally undertake a significant auditing process of the foreign intelligence agency before a State enters into such an agreement. Such an auditing process might entail field visits and consulting local non-governmental organizations on the human rights record of the agency.

3. Non-traditional powers to arrest, detain and interrogate

37. After the events of 11 September 2001, some Governments insisted that clear distinctions between intelligence and law enforcement powers were no longer tenable, arguing that the extraordinary character of the contemporary terrorist threat demands that intelligence agencies acquire new powers to interrogate, arrest and detain people. Giving powers of arrest, detention and interrogation to intelligence agencies is not as such a violation of international law, provided these agencies comply with all relevant human rights standards regarding arrest and detention and with domestic constitutional and other provisions prescribed for ordinary law enforcement agencies.²⁵ However, the Special Rapporteur is concerned that in several countries the power shift from law enforcement agencies to intelligence agencies for countering and preventing terrorist threats was accomplished precisely to circumvent such necessary safeguards in a democratic society, abusing thereby the usually legitimate secrecy of intelligence operations.²⁶ This shift can ultimately endanger the rule of law, as the collection of intelligence and the collection of evidence about criminal acts becomes more and more blurred.²⁷ This leads to a situation where States begin preferring to use undisclosed evidence gathered by intelligence agents in administrative proceedings over attempts to prove guilt beyond reasonable doubt in a criminal trial. Seen in the light of the inherent limitations of intelligence information, preventive measures that deprive a person of his or her liberty must not be based solely on intelligence. In these cases, intelligence has to be turned into concrete evidence and proof after a period of time so that the affected person can challenge the evidence against him or her. If intelligence cannot be transformed into evidence over time, or the State fails to obtain new evidence, the preventive measures need to cease.

²³ See e.g. the Dutch Intelligence and Security Services Act 2002, arts. 36, para. 1 (d), 40, paras. 1 and 42.

²⁴ See e.g. Canadian Security Intelligence Service Act, section 17 (2).

²⁵ See for instance *Ocalan v. Turkey*, ECHR, 12 March 2003, para. 106.

²⁶ See for instance Russia's law "On counter-terrorism action" of 6 March 2006 which transfers ordinary police powers to intelligence agencies while reducing the legal safeguards against the abuse of these powers, for instance in the context of communications monitoring or "stop and search" activities.

²⁷ In the 1970s the Church Committee of the United States Senate had already pointed out that it was exactly the blurring of the distinction between law enforcement and foreign intelligence national security investigations that had led to various abuses outlined in the report, *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, United States Senate, 94th Congress, 1976.

38. In some countries intelligence agencies have legally acquired the power to arrest and detain people who are expected to have information about terrorist activities.²⁸ Preventive detention for public security reasons, including that of interrogating persons for intelligence purposes, may in exceptional circumstances be a proportionate interference with the right to liberty, provided the detention has clear and accessible basis in the law, information on the reasons for detention have been given and the detention is subject to judicial review.²⁹ Detention must not be arbitrary,³⁰ and compensation in the case of unjustified detention must be available.³¹ The Special Rapporteur is concerned about situations where persons are detained for a long period of time for the sole purpose of intelligence-gathering or on broad grounds in the name of prevention. These situations constitute arbitrary deprivation of liberty.³² The existence of grounds for continued detention should be determined by an independent and impartial court. Without delay, the continued detention of such a person triggers a duty for the authorities to establish whether criminal suspicions can be confirmed and, if this is the case, to bring charges against the suspect and to put him on trial. The mere “administrative” detention of a person, for the sole purpose of gathering information would be unlawful.³³

39. The Special Rapporteur is gravely concerned about situations in which intelligence agencies wield arrest and detention powers, but where there is no effective judicial oversight over the actions of the intelligence services, resulting in impunity. In Algeria for example, the military intelligence service (DRS) specializes in detaining and interrogating people who are believed to possess information about the terrorist activities of armed groups acting within Algeria or of international terrorist networks acting abroad. Articles 12 and 16 of the Criminal Procedure Code stipulate that in exercising these functions the DRS operates under the authority of the prosecutor. However, reports indicate that actually the DRS is operating without any civilian oversight.³⁴ Unlike cases where arrests are carried out by police or gendarmerie officers, prosecutors seem not to be informed of arrests carried out by the DRS. Prosecutors apparently do

²⁸ See also the earlier comments of the Special Rapporteur on compulsory hearings in Australia (A/HRC/4/26/Add.3, paras. 31-32 and 46-47).

²⁹ Human Rights Committee, general comment No. 8 (1982) on article 9 (Right to liberty and security of persons), para. 4.

³⁰ See also ECHR, *Fox, Campbell and Hartley v. the United Kingdom*, 30 August 1990, para. 32.

³¹ See for instance, Inter-American Court of Human Rights, report No. 2/97, OEA/Ser.L/V/II.95 Doc. 7 rev. (1997), para. 12.

³² See also the comments of the Special Rapporteur on the situation in Guantanamo Bay (A/HRC/6/17/Add.3, paras. 13-14).

³³ See for instance *Brogan and Others v. the United Kingdom*, ECHR, 19 November 1988, para. 53; *Murray v. the United Kingdom*, ECHR, 28 October 1994, para. 67.

³⁴ Eminent Jurist Panel on Terrorism, Counter-Terrorism and Human Rights, forthcoming report, chapter IV, part 2.2.2.

not use their prerogative to order medical examinations, to visit barracks which are used for *garde à vue* detention, or to verify the records on the arrest, questioning and release of detainees held by the DRS. The Special Rapporteur is concerned that these circumstances substantially increase the risk that persons are arbitrarily detained or will be exposed to torture or other inhuman treatment.

40. The Special Rapporteur is gravely concerned about situations, for instance in Morocco,³⁵ Jordan³⁶ and Pakistan, where the detention and interrogation powers of the intelligence services in counter-terrorism operations and investigations have no clear statutory basis.³⁷ The arrest and detention of persons on grounds which are not clearly established in domestic law is a violation of article 9, paragraph 1, of the International Covenant on Civil and Political Rights. Without such a legal framework there is a danger that intelligence services arrest people on the basis of sheer assumptions, which might be based only on a “guilt by association” pattern.

41. The Special Rapporteur notes that since September 2001 there has been a trend towards outsourcing the collection of intelligence to private contractors.³⁸ While the involvement of private actors can be necessary as a technical matter in order to have access to information (for instance for electronic surveillance), there are reasons to be wary of using contractors to interrogate persons who are deprived of their liberty.³⁹ The combination of a lack of proper training, the introduction of a profit motive into situations which are prone to human rights violations, and the often questionable prospect that such contractors will be subject to judicial and parliamentary accountability mechanisms, justifies the conclusion that intelligence activities that may affect the life, physical integrity or liberty of individuals should remain within the exclusive domain of the State. If States however decide to contract private military and security companies, they should, as a minimum, comply with the Montreux Document on pertinent

³⁵ See Alkarama for Human Rights, *Contribution dans le cadre de l'examen périodique universel de Maroc*, 2007, pp. 2-4; Amnesty International, Morocco, submission to the Universal Periodic Review, 2007, p. 5.

³⁶ Human Rights Watch, *Suspicious Sweeps - The General Intelligence Department and Jordan's Rule of Law Problem* (2006), vol. 18, No. 6 (E), pp. 11-17.

³⁷ Eminent Jurist Panel on Terrorism, Counter-Terrorism and Human Rights, forthcoming report, chapter IV, part 2.2.2.

³⁸ In general, 70 per cent of the intelligence activities of the United States are being outsourced to private actors nowadays. See S. Chesterman, “‘We can’t spy ... if we can’t buy!’: the privatization of intelligence and the limits of outsourcing ‘inherently governmental functions’”, New York University Public Law and Legal Theory Working Papers, No. 82, 2008, p. 2.

³⁹ See for instance *United States v. Passaro* (No. 5:04-CR-211-1, United States District Court for the Eastern District of North Carolina, 17 June, 2004). See also the statements of Central Intelligence Agency (CIA) director Michael Hayden, who has confirmed that contractors “under governmental direction and control” have waterboarded detainees at CIA black sites: Hearing of the United States Senate Select Committee on Intelligence, Annual Worldwide Threat Assessment, 5 February 2008, p. 26.

international legal obligations and good practices for States related to operations of private military and security companies during armed conflict,⁴⁰ which were drafted to apply even in the demanding circumstances of armed conflict.

4. Oversight and review mechanisms of intelligence agencies

42. As the main beneficiary of intelligence information, the executive must effectively supervise and direct the actions of the intelligence agency. These directions should be put in writing,⁴¹ and outline in detail which actions the agencies may and must not carry out vis-à-vis which persons. At stake is not only the oversight and control of the intelligence services but also preventing so-called “plausible deniability”⁴² on behalf of the executive and holding the latter accountable for potential abuses. The Special Rapporteur stresses in this context that authorization for covert actions must be consistent with the human rights obligations of States not only for legal and moral, but also for intelligence reasons.⁴³

43. Authorization for an agency to assassinate, disappear or arbitrarily detain terrorist suspects can never be justified as a legitimate intelligence-led preventive approach to counter-terrorism. Equally, giving powers to arrest and detain high-value detainees in secret detention centres, or allowing inhuman and degrading treatment of suspects under the name of “enhanced interrogation techniques” for the purpose of gathering information⁴⁴ are clear violations of international law. The Special Rapporteur stresses in this regard that the “necessity defence” as it is known in the criminal law of some countries must never serve as a policy or an ex ante justification for the use of prohibited interrogation techniques - even in so-called “ticking bomb” situations.⁴⁵

⁴⁰ A/63/467-S/2008/636.

⁴¹ See for instance: Act CXXV 1995 on National Security, Hungary, section 11; the Dutch Security and Intelligence Services Act 2002, art. 19; and the Canadian Security Intelligence Service Act 1984, section 7 (1) and (2).

⁴² “Plausible deniability” refers to the deliberate creation of power structures and chains of command which are loose and informal enough to enable denying the involvement of the executive when a human rights violation is being disclosed.

⁴³ See for instance United States Senate Armed Services Committee inquiry into the treatment of detainees in United States custody, 12 December 2008, p. xii: “The fact is that senior officials in the United States Government solicited information on how to use aggressive techniques, redefined the law to create the appearance of their legality, and authorized their use against detainees. Those efforts damaged our ability to collect accurate intelligence that could save lives, strengthened the hand of our enemies, and compromised our moral authority.”

⁴⁴ J. Warrick, “CIA tactics endorsed in secret memos”, *Washington Post*, 15 October 2008.

⁴⁵ See A/HRC/6/17/Add.4, paras. 17-21.

44. Several States have devised independent permanent offices, such as inspectors-general, judicial commissioners or auditors, through statutes or administrative arrangements which review whether intelligence agencies comply with their duties. They can act as proactive early warning mechanisms to signal potential problems to the executive, thereby improving accountability. These offices can be required for instance to report at least every six months to the relevant executive bodies on developments and actions of the agencies. To fulfil this function properly such offices must have unrestricted access to all files, premises and personnel of the agency; this is the case for instance in Canada,⁴⁶ South Africa⁴⁷ and various countries in Europe. Specialized and continuous supervision has clear merits compared to ad hoc investigations by general supervisory authorities.⁴⁸ A specific oversight task falls to the national parliament, which in the sphere of intelligence should play its traditional role of holding the executive branch and its agencies accountable to the general public. In practice, there is a diverse range of parliamentary oversight bodies which all have different features, depending on national constitutions and legal traditions.

45. While the Special Rapporteur is aware that it is difficult to identify a universal best practice on this issue, the Norwegian system of parliamentary control is a system that contains at least the elements of best practice as it has an explicit human rights purpose, namely “to ascertain and prevent any exercise of injustice against any person” and to “ensure that activities are kept within the framework of statute law, administrative or military directives and non-statutory law”.⁴⁹ Furthermore, the parliamentary oversight committee is composed of seven members, who are appointed by Parliament but who don’t necessarily have political affiliations. In this way the committee cannot be abused for party political games, a high level of expertise is guaranteed and the credibility of the expert-members is assured. The members are supported by a secretariat of three lawyers and one secretary who all have security clearance. The members have the power to compel the production of evidence to the committee concerning all matters experienced in the course of their duties. In pursuing its duties, the committee has access to the archives and registers, premises, and installations of all branches of the executive and the intelligence agency.

46. There is a risk that with compartmentalized oversight, whereby oversight bodies are assigned to examine just one part of the intelligence community, cross-cutting problems fall through the gaps between oversight bodies. Oversight bodies with a thematic mandate are therefore generally better equipped to address the increasing overlap of functions, cooperation and the sharing of information between various governmental agencies. The Norwegian

⁴⁶ Canadian Security Intelligence Service Act 1984, section 31 (1) and (2).

⁴⁷ South Africa’s Intelligence Services Oversight Act 40 of 1994, section 7 (8) (a).

⁴⁸ See also European Commission for Democracy through Law (Venice Commission), report on the democratic oversight of the security services, CDL-AD(2007)016, para. 142.

⁴⁹ Act relating to the Monitoring of Intelligence, Surveillance and Security Services, February 1995, section 2.

oversight body for instance is charged with reviewing all “intelligence, surveillance and security services carried out by, under the control of, or on the authority of the public administration”.⁵⁰

B. Intelligence cooperation

47. When it became clear, soon after the events of 11 September 2001, that the attacks were prepared in part in Western Europe, and that some of the terrorists apparently involved in the attacks were under observation by, inter alia, the German and French intelligence agencies, the need for more effective and coordinated cooperation between intelligence agencies was widely acknowledged.⁵¹ The benefit of sharing intelligence is clear: no State has an all-seeing “Eye of Providence” which enables it to know all potential information which might be relevant for its national security interests.

48. This legitimate cooperation often poses accountability problems. This is mainly because on the one hand domestic accountability mechanisms only tend to take into account the actions of domestic agencies because their mandate does not cover the cooperation of their agencies with third partners or, where they are mandated to scrutinize cooperation, these powers are often very limited. On the other hand, two key concepts that underlie most top secret intelligence-sharing agreements, namely the “need to know” approach to intelligence distribution⁵² and the policy of “originator control”,⁵³ increase the possibility that many countries, including liberal democracies opposed to torture, become complicit in international crimes. Because of the desire to maintain cooperation from (especially more powerful) foreign agencies, intelligence services have limited incentives to request clarification on how certain information has been obtained or to ensure that the information they share will not be used in a manner that leads to human rights violations. At the same time domestic oversight bodies are often powerless to oversee the adherence of a foreign intelligence agency to any conditions attached to outgoing information.

⁵⁰ Ibid., section 1.

⁵¹ Security Council resolutions 1373 (2001), para. 3 (a) and (b), and 1465 (2003), para 3; EU Declaration on combating terrorism, 2004, para. 9; Association of Southeast Asian Nations (ASEAN) Convention on Counter Terrorism, 2007, art. VI (h).

⁵² Under the “need to know” principle, “individuals should have access to classified information only when they need the information for their work, and access should never be authorized ‘merely because a person occupies a particular position, however senior’”, NATO Security Committee, *A Short Guide to the Handling of Classified Information* (Brussels, NATO Archives, 22 August 1958, AC/35-WP/14), quoted in A.S. Roberts, “Entangling alliances: NATO’s security policy and the entrenchment of State secrecy”, *Cornell International Law Journal*, vol. 36, No. 2 (2003), p. 337.

⁵³ Under the principle of “originator control” - also often referred to as the “third party rule” - intelligence agencies only send intelligence under the understanding that neither the information nor its source will be disclosed without the prior consent of the entity which provided it.

49. Intelligence cooperation is often practised in the context of multilateral organizations such as NATO or the Shanghai Cooperation Organisation. The Special Rapporteur is concerned that the secrecy and security of information policies that are adopted by States within these multilateral frameworks provide an insurmountable wall against independent investigations into human rights violations. For instance, the report of the Committee on Legal Affairs and Human Rights of the Council of Europe Parliamentary Assembly (rapporteur Dick Marty) gives credible information that bilateral (secret) agreements that allowed for blanket overflight rights, access to ports and military bases for covert Central Intelligence Agency (CIA) operations, including secret detentions and renditions, were developed around “permissive” NATO authorizations agreed on 4 October 2001.⁵⁴ In the Shanghai Cooperation Organisation cooperation between secret services is exercised without any oversight. A service merely requests “assistance”⁵⁵ from another service upon which the receiving State “shall take all necessary measures to ensure a prompt and most complete execution of the request”.⁵⁶ According to article 11.4 of the Shanghai Convention on Combating Terrorism, Separatism and Extremism, any information on the means used by agencies in order to provide assistance to another agency “shall not be subject to disclosure”.

50. To counter the lack of accountability in intelligence cooperation, cooperation between national oversight bodies should be enhanced. Existing initiatives in this field, such as the biannual International Intelligence Review Agencies Conference or the ad hoc meetings of parliamentary intelligence oversight committees of EU member and candidate countries, are a first step in the right direction but happen too infrequently and are currently limited to a too small group of States. The Special Rapporteur supports the idea, developed by Belgian Standing Committee I, of setting up a permanent knowledge-sharing platform for (parliamentary) review bodies of intelligence services, where best practices on legislation, jurisprudence and general developments in the field can be shared, thereby supporting the professionalization of the review bodies of Member States.⁵⁷ Such a platform might even be extended to operational matters, whereby the collaboration on inquiries and the exchange of information could lead into a form of “joint oversight”.⁵⁸

⁵⁴ *Secret detentions and illegal transfers of detainees involving Council of Europe member States: second report*, explanatory memorandum, Committee on Legal Affairs and Human Rights, Council of Europe Parliamentary Assembly, June 2007, paras. 11, 39 and 105.

⁵⁵ The State just has to describe “the contents” of the required assistance (Shanghai Convention on Combating Terrorism, Separatism and Extremism, art. 8, para. 3). This can include interrogating, detaining and extraditing persons.

⁵⁶ *Ibid.*, art. 9.

⁵⁷ A further model for such cooperation can be found in the periodic meetings of police oversight bodies in European States.

⁵⁸ H. Born, “International intelligence cooperation: the need for networking accountability”, DCAF, 2007.

1. Joint operations

51. The Special Rapporteur remains deeply troubled that the United States has created a comprehensive system of extraordinary renditions, prolonged and secret detention, and practices that violate the prohibition against torture and other forms of ill-treatment. This system required an international web of exchange of information and has created a corrupted body of information which was shared systematically with partners in the war on terror through intelligence cooperation, thereby corrupting the institutional culture of the legal and institutional systems of recipient States.

52. While this system was devised and put in place by the United States, it was only possible through collaboration from many other States. There exist consistent, credible reports suggesting that at least until May 2007 a number of States facilitated extraordinary renditions in various ways. States such as Bosnia and Herzegovina, Canada, Croatia, Georgia, Indonesia, Kenya, the former Yugoslav Republic of Macedonia, Pakistan and the United Kingdom of Great Britain and Northern Ireland have provided intelligence or have conducted the initial seizure of an individual before he was transferred to (mostly unacknowledged) detention centres in Afghanistan, Egypt, Ethiopia, Jordan, Pakistan, Morocco, Saudi Arabia, Yemen, Syria, Thailand, Uzbekistan, or to one of the CIA covert detention centres, often referred to as “black sites”. In many cases, the receiving States reportedly engaged in torture and other forms of ill-treatment of these detainees.

53. The Special Rapporteur reminds States that they are responsible where they knowingly engage in, render aid to or assist in the commission of internationally wrongful acts, including violations of human rights.⁵⁹ Accordingly, grave human rights violations by States such as torture, enforced disappearances or arbitrary detention should therefore place serious constraints on policies of cooperation by States, including by their intelligence agencies, with States that are known to violate human rights. The prohibition against torture is an absolute and peremptory norm of international law.⁶⁰ States must not aid or assist in the commission of acts of torture, or

⁵⁹ General Assembly resolution 56/83, annex, International Law Commission draft articles on responsibility of States for internationally wrongful acts, arts. 4 and 16. See also *Yearbook of the International Law Commission, 2001*, vol. II, Part Two, p. 66, “In such a case, the assisting State will only be responsible to the extent that its own conduct has caused or contributed to the internationally wrongful act.” Article 16 reflects a rule of customary international law. See International Court of Justice (ICJ), *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgement of 26 February 2007, para. 420.

⁶⁰ The obligation to protect against and sanction torture is an obligation erga omnes, an obligation owed to all States. See International Criminal Tribunal for the former Yugoslavia (ICTY), *Prosecutor v. Furundzija* (Case No. IT-95-17/1-T 1988); *Barcelona Traction, Light and Power Company Limited (Belgium v. Spain)*, ICJ reports 1970.

recognize such practices as lawful, including by relying on intelligence information obtained through torture.⁶¹ States must introduce safeguards preventing intelligence agencies from making use of such intelligence.⁶²

2. Participation in interrogations

54. The Special Rapporteur is concerned about the participation of foreign agents in the interrogation of persons held in situations that violate international human rights standards. The difference that some Governments make between intelligence and law enforcement personnel is of limited relevance, as the active participation through the sending of interrogators⁶³ or questions,⁶⁴ or even the mere presence of intelligence personnel at an interview with a person who is being held in places where his rights are violated,⁶⁵ can be reasonably understood as implicitly condoning such practices.⁶⁶ The continuous engagement and presence of foreign

⁶¹ General Assembly resolution 56/83, annex, International Law Commission draft articles on responsibility of States for internationally wrongful acts, arts. 40-41.

⁶² As Justice Neuberger states: “(...) even by adopting the fruits of torture, a democratic State is weakening its case against terrorists, by adopting their methods, thereby losing the moral high ground an open democratic society enjoys”. Lord Justice Neuberger (dissenting) in *A and Ors v. Secretary of State for the Home Department*, [2004] EWCA Civ 1123 (11 August 2004), para. 497.

⁶³ Evidence proves that Australian, British and United States intelligence personnel have themselves interviewed detainees who were held incommunicado by the Pakistani ISI in so-called safe houses, where they were being tortured. Many countries (Bahrain, Canada, China, France, Germany, Italy, Jordan, Libya, Morocco, Pakistan, Saudi Arabia, Spain, Tajikistan, Tunisia, Turkey, United Kingdom, Uzbekistan) have sent interrogators to Guantanamo Bay as well (see Center for Constitutional Rights, “Foreign interrogators in Guantanamo Bay”, available at http://ccrjustice.org/files/Foreign%20Interrogators%20in%20Guantanamo%20Bay_1.pdf).

⁶⁴ German and Canadian intelligence agencies provided questions to Syrian Military Intelligence in the cases of Muhammad Zammar and Abdullah Almalki. Both detainees were tortured afterwards while in Syrian custody. See Amnesty International, *United States of America: Below the radar - Secret flights to torture and “disappearance”*, 5 April 2006, pp. 18-19; *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmed Abou-Elmaati and Muayyed Nureddin*, 2008, p. 411.

⁶⁵ United Kingdom intelligence personnel for instance conducted or witnessed just over 2,000 interviews in Afghanistan, Guantanamo Bay and Iraq. See Intelligence and Security Committee, *The Handling of Detainees by UK Intelligence Personnel in Afghanistan, Guantanamo Bay and Iraq*, 2005, para. 110.

⁶⁶ See footnote 61 above.

officials has in some instances constituted a form of encouragement or even support.⁶⁷ In the view of the Special Rapporteur, the responsibility of the receiving State may be triggered also by even more passive and geographically distant forms of creating a demand for intelligence information obtained through internationally wrongful means. Therefore, the Special Rapporteur believes that the active or passive participation by States in the interrogation of persons held by another State constitutes an internationally wrongful act if the State knew or ought to have known that the person was facing a real risk of torture⁶⁸ or other prohibited treatment, including arbitrary detention.⁶⁹

3. Sending and receiving intelligence for operational use

55. The Special Rapporteur emphasizes that not only active participation in interrogations where people are tortured would constitute a violation of human rights law, but also taking advantage of the coercive environment. At a minimum, States which know or ought to know that they are receiving intelligence from torture or other inhuman treatment, or arbitrary detention, and are either creating a demand for such information or elevating its operational use to a policy, are complicit in the human rights violations in question.⁷⁰ The Special Rapporteur believes that reliance on information from torture in another country, even if the information is obtained only for operational purposes, inevitably implies the “recognition of lawfulness” of such practices and therefore triggers the application of principles of State responsibility.⁷¹ Hence, States that receive information obtained through torture or inhuman and degrading treatment are complicit in the commission of internationally wrongful acts. Such involvement is also irreconcilable with the obligation erga omnes of States to cooperate in the eradication of torture.

56. States also claim that in practice it is difficult to assess under what conditions the information has been gathered: intelligence is usually not shared as raw intelligence, but as a refined product. While the Special Rapporteur recognizes that this is done as a matter of convenience, he is concerned that this practice also is maintained in order to give intelligence services the possibility of denying responsibility for the use of information that has been obtained in breach of international law.

⁶⁷ This is particularly the case if - as alleged in Pakistan - persons are held at the request and with the approval of foreign agents. Equally, the Arar Inquiry considered the sending of a team of investigators to speak to the Syrian Intelligence Services SMI to be highly problematic.

⁶⁸ See analogously, ICTY Furundzija Appeal Judgement (21 July 2000), paras. 115-120 and General Assembly resolution 56/83, annex, International Law Commission draft articles on responsibility of States for internationally wrongful acts, arts. 40-41.

⁶⁹ See also Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment, principle 21, para. 1.

⁷⁰ See also the findings of the Eminent Jurist Panel on Terrorism, Counter-Terrorism and Human Rights, forthcoming report, chapter IV, part 3.2.

⁷¹ General Assembly resolution 56/83, annex, International Law Commission draft articles on responsibility of States for internationally wrongful acts, arts. 40-41.

57. The Special Rapporteur is equally concerned about the supply of information to foreign intelligence services, when there are no adequate safeguards attached to the further distribution of such information among other governmental agencies in the receiving State, such as law enforcement and immigration agencies which have the power to arrest and detain a person. In the Arar case, for example, the information sharing between the United States and Canada was on the basis of a purely verbal “free flow” agreement: intelligence was to be exchanged in real time through direct communication among the various agencies involved.⁷² In this agreement, the Royal Canadian Mounted Police abandoned the privacy policies that ordinarily would have governed national security investigations, which resulted in the sharing of inaccurate and misleading information and in broader sharing of information than was usually the case. It was this information that led the United States Immigration and Naturalization Service to conclude that Arar was a member of Al-Qaida after which he was deported to Syria where he was subsequently tortured.

C. Ex post facto accountability and the right to an effective remedy

58. Ex-ante control and oversight mechanisms are important in preventing and discovering human rights violations by intelligence agencies in the fight against terrorism. Equally important, however, is the duty of the State to create a framework that enables an independent investigation into human rights violations by intelligence agencies after a complaint has been received in order, firstly, to establish the facts and, secondly, to hold intelligence agencies and the executive accountable for their actions. The Special Rapporteur is concerned in this context about the adoption of indemnity/impunity clauses which result in impunity for intelligence agents.⁷³ Such indemnity clauses can bar effective access to court and violate the human right to an effective remedy.

The abuse of State secrecy provisions

59. While the Special Rapporteur recognizes that States may limit the disclosure to the general public of specific information which is important for the protection of national security, for instance about the sources, identities and methods of intelligence agents, he is nevertheless worried by the increasing use of State secrecy provisions and public interest immunities for instance by Germany, Italy, Poland, Romania, the former Yugoslav Republic of Macedonia, the United Kingdom or the United States to conceal illegal acts from oversight bodies or judicial authorities, or to protect itself from criticism, embarrassment and - most importantly - liability.

⁷² See Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, Report of the Events Relating to Maher Arar, Factual Background vol. I, p. 38; F. Bignami, “Towards a right to privacy in transnational intelligence networks”, *Michigan Journal of International Law*, vol. 28, No. 3 (2007), pp. 675-676.

⁷³ See for instance Algeria, articles 45 and 46 of Ordinance 06-01 of 27 February 2006 (implementing the Charter for Peace and Reconciliation) grant impunity to members of the security forces and even criminalize criticism of State agents with years of imprisonment.

60. The human rights obligations of States, in particular the obligation to ensure an effective remedy, require that such legal provisions must not lead to a priori dismissal of investigations, or prevent disclosure of wrongdoing, in particular when there are reports of international crimes or gross human rights violations.⁷⁴ The blanket invocation of State secrets privilege with reference to complete policies, such as the United States secret detention, interrogation and rendition programme⁷⁵ or third-party intelligence (under the policy of “originator control” (see paragraph 48 above)) prevents effective investigation and renders the right to a remedy illusory. This is incompatible with article 2 of the International Covenant on Civil and Political Rights. It could also amount to a violation of the obligation of States to provide judicial assistance to investigations that deal with gross human rights violations and serious violations of international humanitarian law.⁷⁶

61. In order to enable effective investigations to take place, the Special Rapporteur is of the opinion that robust whistle-blower protection mechanisms for intelligence agents and other informers are crucial in order to break illegitimate rings of secrecy. Reliable factual information about serious human rights violations by an intelligence agency is most likely to come from within the agency itself. In these cases, the public interest in disclosure outweighs the public interest in non-disclosure. Such whistle-blowers should firstly be protected from legal reprisals and disciplinary action when disclosing unauthorized information. Secondly, independent oversight mechanisms must be able to give whistle-blowers and informants the necessary protections, which could be modelled on the witness protection programmes of the International Criminal Tribunal for the former Yugoslavia, the International Criminal Tribunal for Rwanda, the Special Court for Sierra Leone and the International Criminal Court.

62. The Special Rapporteur emphasizes the important work many investigative journalists and non-governmental organizations do around the world in uncovering human rights violations by intelligence agencies. Often accountability is not triggered by formal mechanisms, but through

⁷⁴ See for instance Inter-American Court of Human Rights, *Myrna Mack-Chang v. Guatemala*, judgement, 25 November 2003, para. 180; ECHR, *Imakayeva v. Russia*, judgement, 9 November 2006.

⁷⁵ In *El-Masri v. Tenet*, the Government filed a declaration by CIA director Porter J. Goss which argued that the claims alleged by rendition victim El-Masri would force the CIA to admit or deny the existence of clandestine CIA activities, and that therefore dismissal of the suit was the only proper outcome on the basis of State secrets privilege. (Assertion of a Formal Claim of State Secrets Privilege and Request for Expedited Consideration, 8 March 2006, United States District Court - Eastern District of Virginia, Case No. 1:05-cv-1417-TSE-TRJ). See also the declarations of James B. Comey, acting Attorney General and Tom Ridge, Secretary of the U.S. Department of Homeland Security, 18 January 2005 in *Arar v. Ashcroft* C.A. No. 04-CV-249-DGT-VVP.

⁷⁶ See principle 12 of the Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law, adopted by the General Assembly in resolution 60/147.

revelations by these actors. In order for the press to perform their vital function as an external, unofficial control mechanism, robust freedom of information laws and laws protecting journalists' confidential sources⁷⁷ are absolutely necessary. States must limit prosecutions for breaching secrecy provisions to their officials,⁷⁸ introduce a mandatory public interest test and oblige the courts to consider the public interest value when it comes to the publication of official State secrets.

63. In all cases judges must be the ultimate arbitrators in assessing the merits of the State secrecy claim when serious human rights violations are at stake. Their rulings may allow the disclosure of the disputed information to the public or to a terrorist suspect and his lawyer in legal proceedings. In order to test secrecy claims in the latter case, a judicial body should have access to the actual evidence a Government is seeking to protect, rather than mere summaries or declarations provided by the Government. Where there are reasons for excluding elements that can justifiably be considered as State secrets, courts should consider counter-balancing measures for not making available such information in a public hearing, for instance by limiting access to the information to the (if necessary, security cleared) lawyer of the suspect. Only when strictly necessary could a judge decide to make a distinction between disclosing the provenance of the evidence (the source and the method used) and the content of the information, which should always be open to challenge.

III. CONCLUSIONS AND RECOMMENDATIONS

A. Conclusions

64. The increased powers of intelligence services to conduct measures that seriously interfere with individuals' rights, as well as the increasing relevance of intelligence for legal and administrative actions, make it essential that adequate accountability mechanisms are put in place to prevent human rights abuses. Under international human rights law, States are under a positive obligation to conduct independent investigations into alleged violations of the right to life, freedom from torture or other inhuman treatment, enforced disappearances or arbitrary detention,⁷⁹ to bring to justice those responsible for such acts, and to provide reparations where

⁷⁷ In Belgium, for instance, the Law on the protection of journalistic sources of 7 April 2005 (Moniteur Belge, 27 April 2005) permits journalists and media employees explicitly "to keep their sources secret" (art. 3).

⁷⁸ See in this context the "Cicero" ruling of the German Constitutional Court in 2007, which stated that journalists cannot be legitimately accused of betrayal of State secrets for publishing classified information obtained from informers. See BVerfG, 1 BvR 538/06 of 27.2.2007, Absatz-Nr. (1-82), available at http://www.bverfg.de/entscheidungen/rs20070227_1bvr053806.html.

⁷⁹ *Aydin v. Turkey* (1997) 25 ECHR 251; Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, arts. 5, 6, 12 and 13; Human Rights Committee, general comment No. 31 (2004) on the Nature of the General Legal Obligation Imposed on States Parties to the Covenant, paras. 15 and 18.

they have participated in such violations. States retain this positive obligation to protect human rights where they grant privileges within their national territory to another State, including to intelligence services.

B. Recommendations

For legislative assemblies

65. **The Special Rapporteur recommends that any interference with the right to privacy, family, home or correspondence by an intelligence agency should be authorized by provisions of law that are particularly precise, proportionate to the security threat, and offer effective guarantees against abuse. States should ensure that competent authorities apply less intrusive investigation methods than special investigation techniques if such methods enable a terrorist offence to be detected, prevented or prosecuted with adequate effectiveness. Decision-making authority should be layered so that the greater the invasion of privacy, the higher the level of necessary authorization. Furthermore, in order to safeguard against the arbitrary use of special investigative techniques and violations of human rights, the use of special investigative techniques by the intelligence agencies must be subject to appropriate supervision and review.**

66. **There should be a domestic legal basis for the storage and use of data by intelligence and security services, which is foreseeable as to its effects and subject to scrutiny in the public interest. The law should also provide for effective controls on how long information may be retained, the use to which it may be put, and who may have access to it, and ensure compliance with international data protection principles in the handling of information. There should be audit processes, which include external independent personnel, to ensure that such rules are adhered to.**

67. **The Special Rapporteur also recommends the adoption of legislation that clarifies the rights, responsibilities, and liability of private companies in submitting data to government agencies.**

68. **Parliamentary oversight committees, ad hoc parliamentary inquiry committees, royal commissions, etc. should have far-reaching investigative powers, access to the archives and registers, premises, and installations of the executive and the agency, in order to fulfil their domestic oversight function. These bodies should also be able to proactively investigate the relationship of a domestic agency with a particular State or service, or all exchanges of information with foreign cooperating services pertaining to a particular case. After their inquiry these bodies should produce simultaneously a confidential report for the executive and a separate report for public disclosure.**

69. **The Special Rapporteur supports the recommendation of the Eminent Jurist Panel on Counter-Terrorism, Terrorism and Human Rights that intelligence agencies should not perform the functions of law enforcement personnel.⁸⁰ If, despite the potential for abuse,**

⁸⁰ Eminent Jurist Panel on Counter-Terrorism, Terrorism and Human Rights, 2009, forthcoming report, chapter IV, part 5.

intelligence services are nonetheless accorded powers of arrest, detention and interrogation, the Special Rapporteur urges that they be under the strict and effective control of ordinary civilian authorities and operate with full respect for international human rights law.

70. Intelligence cooperation must be clearly governed by the law (including human rights safeguards) and by transparent regulations, authorized according to strict routines (with proper “paper trails”) and controlled or supervised by parliamentary or expert bodies.

For the executive power

71. The executive should have effective powers of control, provided for in law, over the intelligence agencies and have adequate information about their actions in order to be able to effectively exercise control over them. The minister responsible for the intelligence and security services should therefore have the right to approve matters of political sensitivity (such as cooperation with agencies from other countries) or undertakings that affect fundamental rights (such as the approval of special investigative powers, whether or not additional external approval is required from a judge).

72. The Special Rapporteur urges all relevant authorities of countries that have allegedly participated in extraordinary renditions, torture, disappearances, secret detentions or any other serious human rights violation to investigate fully any wrongful acts of intelligence agencies committed on their territory. States must ensure that the victims of such unlawful acts are rehabilitated and compensated. States must also stop transferring anyone to the custody of the agents of another State, or facilitating such transfers, unless the transfer is carried out under judicial supervision and in line with international standards.

73. The Special Rapporteur recommends that States insert a clause in their intelligence-sharing agreements which makes the application of an agreement by a party subject to scrutiny by its review bodies and which declares that the review bodies of each party are competent to cooperate with one another in assessing the performance of either or both parties.⁸¹

For intelligence agencies

74. The Special Rapporteur recommends that classified information may be shared with other intelligence agencies only when it contains a written caveat, which limits the further distribution of such information among other governmental agencies in the receiving State, such as law enforcement and immigration agencies, which have the power to arrest and detain a person. In this regard, the Special Rapporteur advises that sanctions against a person should not be based on foreign intelligence, unless the affected party can effectively challenge the credibility, accuracy and reliability of the information and there are credible grounds to believe that the information is accurate and reliable.

⁸¹ See C. Forcese, *The Collateral Casualties of Collaboration - the Consequence for Civil and Human Rights of Transnational Intelligence Sharing*, conference paper for the DCAF workshop on accountability of international intelligence cooperation, Oslo, 17 October 2008.

75. The Special Rapporteur urges Member States to reduce to a minimum the restrictions of transparency founded on concepts of State secrecy and national security. Information and evidence concerning the civil, criminal or political liability of State representatives, including intelligence agents, for violations of human rights must not be considered worthy of protection as State secrets. If it is not possible to separate such cases from true, legitimate State secrets, appropriate procedures must be put into place ensuring that the culprits are held accountable for their actions while preserving State secrecy.

76. The Special Rapporteur recommends that intelligence agencies develop internal and international training programmes in how to comply with human rights in their operations. Such training should be based on the idea that compliance with human rights is a part of professional qualifications, and a source for professional pride, for any intelligence officer.

77. A codified regulation should be in place which guarantees appropriate support and security for whistle-blowers within the intelligence agencies.

For the Human Rights Council

78. The Special Rapporteur recommends the elaboration and adoption of an instrument such as guidelines for human rights compliance and best practice by intelligence agencies.⁸²

⁸² See similarly, Code of Conduct for Law Enforcement Officials adopted by the General Assembly in resolution 34/169.