International Centre for
Counter-Terrorism - The Hague

Towards the intelligent use of intelligence: *Quis Custodiet ipsos Custodes?*

Dr. Bibi van Ginkel LL.M.

ICCT Research Paper
August 2012

Abstract

In this ICCT Research Paper Dr. Bibi van Ginkel examines the role of the exchange of intelligence between states, the applicable human rights framework, and the dilemmas involved. Over the last ten years, more and more significance has been accorded to intelligence on a global scale. This is reflected in a considerable upgrade of security structures and their resourcing. In dealing with global and transnational security risks, there is also an increasing need for building intelligence relations among countries. At the same time, the focus of traditional law enforcement is moving towards preventive mechanisms that are mainly intelligence-driven. Although indeed, it is better to prevent terrorism from taking place than to deal with the consequences afterwards, the challenge is to ensure human rights as well as accountability for its violations, while recognizing the important role of intelligence, including its need for confidentiality. In case of sharing intelligence between states, every state bears the responsibility to protect the safety as well as the democratic principles and the rule of law. This paper begins with the question *Quis custodiet ipsos custodes*? Or, *who guards the guardians*? It explores the above mentioned topics and the final section concludes with a series of policy recommendations for the intelligent use of intelligence.

About the Author

Dr. Bibi van Ginkel LL.M. is a Research Fellow at the International Centre for Counter-Terrorism – The Hague, and a Senior Research Fellow at the Clingendael Security and Conflict Programme (CSCP) of the Netherlands Institute of International Relations. She studied International and European Law (Netherlands). In June 2010, she defended her PhD thesis The Practice of the United Nations in Combating Terrorism from 1946-2008; Questions of Legality and Legitimacy. Before working at the Clingedael Institute, she taught International and European Law at Utrecht University. She coordinated the research project 'Ethical Justness of European Counter-Terrorism Measures', which was part of the Sixth Framework Programme of the European Commission. She is a member of the Peace and Security Committee of the Dutch Advisory Council on International Affairs. Additionally, she is General Secretary of the Daily Board of the Netherlands Helsinki Committee. Her areas of interest include the security related aspects of law, such as terrorism, piracy and the employment of Private Security Companies.

About ICCT - The Hague

The International Centre for Counter-Terrorism (ICCT) – The Hague is an independent knowledge centre that focuses on information creation, collation and dissemination pertaining to the preventative and international legal aspects of counter-terrorism. The core of ICCT's work centres on such themes as de- and counter-radicalisation, human rights, impunity, the rule of law and communication in relation to counter-terrorism. Functioning as a nucleus within the international counter-terrorism network, ICCT – The Hague endeavours to connect academics, policymakers and practitioners by providing a platform for productive collaboration, practical research, exchange of expertise and analysis of relevant scholarly findings. By connecting the knowledge of experts to the issues that policymakers are confronted with, ICCT – The Hague contributes to the strengthening of both research and policy. Consequently, avenues to new and innovative solutions are identified, which will reinforce both human rights and security.

Contact

ICCT – The Hague
Koningin Julianaplein 10
P.O. Box 13228
2501 EE, The Hague
The Netherlands

T +31 (0)70 800 9531
E info@icct.nl

All papers can be downloaded free of charge at **www.icct.nl**
Stay up to date with ICCT, follow us online on Facebook, Twitter and LinkedIn

1. Introduction

The Latin phrase 'Quis Custodiet ipsos custodes?' is traditionally attributed to the Roman poet Juvenal from his *Satires* (Satire VI, lines 347–8), which is literally translated as "Who will guard the guards themselves?" This phrase, in combination with the concept developed in Plato's *Republic*[1] which relates to the problem on how to ensure that persons entrusted to guard the interests of the state or society do so faithfully, is often used to underline the principle of the Trias Politica. It thus relates to the challenge that while the guards are tasked to keep society safe, it is important that the system does not run the risk of becoming corrupt by overzealous officers of the state, who might become interested in strengthening or even preserving their own position at all costs. Indeed, if the guardians are the secret service, this would, after all, undermine the fundamentals of society. Such a society would creep towards a police state with no democratic control over the executive power and would have no respect for the rule of law. A democratic state based on the rule of law should therefore install checks and balances into its systems to monitor the respect of the mandates attributed to guardians of the state.

These guardians obviously deal with the important task of preserving our security, for which specific powers are attributed. When the guardians are the intelligence agencies, and the security risks have a transnational character such as terrorism, cooperation between the guardians is indeed the obvious next step. However, the protection of democratic values is just as well a key duty of the state and its guardians, and this should therefore translate into the way in which states act when it comes to sharing intelligence. The focus of this paper is on the dilemmas of sharing intelligence information, the risk of undermining the democratic values and human rights principles, and the way in which checks and balances can be incorporated in the cooperation agreements.

In 2011, ICCT organised an Expert Meeting on the use of intelligence information in terrorism-related criminal court cases.[2] The focus of this meeting was to learn from various national approaches in dealing with the use of intelligence in court cases, and the legal guarantees and frameworks in place to facilitate it. The meeting looked at several case studies including: The Netherlands, France, the United Kingdom and Canada. These states have all set up systems to enable the use of intelligence in criminal court cases while – at least in theory – respecting the principles that follow from the international legal framework. The differences in procedures and legal guarantees in place between the different states, however, were quite remarkable. One question that qualifies for further research, is the issue of sharing and exchange of intelligence between states, particularly in light of the guarantees that need to be upheld in national criminal procedures. This question becomes especially salient when the intelligence comes from states that do not share the same standard of respect for human rights.

Clearly, the purpose of gathering intelligence, whether through a state's own activities or because it was shared by foreign intelligence services, is not primarily to use this information for building criminal cases, but it can and should never be excluded beforehand. With the focus of traditional law enforcement moving towards preventive actions and interventions that are mainly intelligence-driven, this possibility becomes an even bigger issue to take into account. Although, it is indeed better to prevent terrorism from taking place than to deal with the consequences afterwards, the challenge is to ensure the upholding of human rights as well as accountability in case of violations, while recognising the important role of intelligence, including its need for confidentiality. Sharing intelligence between states should be on the basis of absolute trust in legal guarantees and basic human rights being upheld during the process of gathering intelligence by the foreign counterpart.

---

[1] In Plato's *Republic,* a perfect society is discussed by Socrates, who proposed a guardian class to protect the society, but who also warned that the guardians might be manipulated to guard themselves against themselves via a deception often called the 'noble lie'.

[2] The report of this expert meeting, as well as the research paper on this topic can be found on the ICCT website: http://www.icct.nl/activities/past-events/em-intelligence-in-court, last visited on 22 August 2012.

This paper will first look at the increased role of the exchange of intelligence between states in preventing and countering terrorism. Next, the applicable human rights framework, and the dilemmas involved will be dealt with. Finally, it will conclude with some recommendations for the intelligent use of intelligence. [3]

2. Exchange of intelligence

In a study on intelligence practice and democratic oversight the Geneva Centre for the Democratic Control of the Armed Forces concluded that the events of 9/11 have provoked reforms in the use of intelligence.[4] Sepper points out that some contemporary intelligence networks date back to the Cold War, and are thus not new at all. In the aftermath of 9/11, however, these networks were "expanded to include some unlikely and otherwise hostile intelligence partners."[5] Conditions under which intelligence is gathered have changed and the basic structure of intelligence services in democracies have been questioned. This is partly due to the new threat caused by non-state actors, the fact that the majority of threats have a transnational character, and the asymmetrical nature of these threats.[6] Another reason is that due to technological developments it has become easier to acquire intelligence.[7] Moreover, more often governments hire private companies to gather intelligence. As a result of the changes in practice of most intelligence services, and the new laws installed to amend their mandates, it has become substantially easier for authorities to get access to information on individuals, which is often gathered by third parties (schools, employers, financial institutions, health care providers, etc.). Intelligence services are also putting citizens under surveillance more often, and without prior notification. This makes it less likely that they are held accountable by any oversight body, simply because the target of the surveillance is not aware of it and therefore does not start an investigation into the legality and legitimacy of the surveillance.

The former United Nations (UN) Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Martin Scheinin, also came to the conclusion that a new significance has been accorded to intelligence on a global scale and is also reflected in a considerable upgrade of security structures and their resourcing.[8] According to Staberock, this is demonstrated by increased powers and controls throughout the 'intelligence cycle',[9] especially:

- increased intelligence collection with lower thresholds and safeguards, including judicial supervision;
- increased intelligence sharing both nationally and internationally;

---

[3] The Eminent Jurists Panel advised to set up a framework for 'intelligent intelligence', which finds its basis in human rights law, and in which security objectives and protecting rights in relation to intelligence activities can be addressed and resolved. Report of the Eminent Jurists Panel on Terrorism, Counter-Terrorism and Human Rights, 'Assessing Damage, Urging Action', ICJ, Geneva, 2009.

[4] Geneva Centre for the Democratic Control of the Armed Forces (DCAF), Intelligence Working Group, 'Occasional Papers no.3: Intelligence Practice and Democratic Oversight – a Practitioner's View', July 2003.

[5] Elisabeth Sepper, 'Democracy, Human Rights, and Intelligence Sharing', in: *Texas International Law Journal,* Vol. 46, 2010, pp. 151-207, at 154-155.

[6] Geneva Centre for the Democratic Control of the Armed Forces (DCAF), Intelligence Working Group, 'Occasional Papers no.3: Intelligence Practice and Democratic Oversight – a Practitioner's View', July 2003,. p. 70.

[7] Quirine Eijkman, *Counter-Terrorism, Technology and Transparency: Reconsidering state accountability?*, ICCT-Paper, 2 February 2012, http://www.icct.nl/download/file/ICCT-de-Graaf-EM-Paper-Terrorism-Trials-as-Theatre.pdf, last visited on 28 August 2012.

[8] Report of the (former) UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while countering terrorism, Martin Scheinin', 4 February 2009, UN Doc A/HRC/10/3.

[9] According to DCAF, the intelligence cycle usually comprises five steps: (1) planning and direction; (2) collection; (3) processing; (4) production and analysis; and (5) dissemination. *Geneva Centre for the Democratic Control of the Armed Forces (DCAF), Intelligence Working Group, 'Occasional Papers no.3: Intelligence Practice and Democratic Oversight – a Practitioner's View', July 2003, p.* 18.

- increased intelligence powers of arrest, detention, and interrogation traditionally confined to law enforcement authorities;
- increased use of intelligence as the basis of executive actions or a range of intelligence based preventive administrative sanctions; and
- decreased accountability for wrongdoing, human rights violations, or criminal conduct through the invocation of expansive notions of state secrecy or national security doctrines and limited judicial review.[10]

In dealing with global and transnational security risks such as terrorism, there is an increasing need for building intelligence relations among countries, and the frequency with which these have been used has also expanded. In 2010, the Canadian Security Intelligence Service (CSIS), a service with little independent ability to collect intelligence abroad, had more than 250 information sharing agreements with foreign security and intelligence organisations, while the Central Intelligence Agency (CIA) had connections with more than 400 agencies worldwide.[11] Obviously, the advantage of intelligence sharing and exchange is to create a better position for policymakers to develop well-informed security decisions in a timely manner. After all, no state can know all of the potential information that is relevant for its national security.

The character of cooperation between intelligence services of different states can take different forms. It can relate to the permission to gather information on the territory of a state, the gathering of information in one's own state on the request of another state, the interrogation of suspects, the sharing of intelligence information and analysis, and the cooperation in certain operations.

Exchange of intelligence between states is based on a few principles, such as *quid pro quo*, the exclusivity of the shared information (meaning neither the information nor the source can be shared with third parties without prior consent of the entity that provided the information) also known as the policy of 'originator control' or the 'third party rule', the 'need to know' approach to intelligence distribution, and more generally: trust. The fact that all states have to abide by international law, and that hence limits exist on the legality of the use or exchange of intelligence has, so far, not translated into an adopted set of clear principles and rules that are part of any agreement between states on the exchange of intelligence.

The networks of intelligence sharing and the underlying agreements are mostly opaque. Although the existence of some networks between states and agencies has been revealed, the essential elements, such as the partners, the *modus operandi* and/or the underlying agreement itself remain top secret,[12] amongst other considerations based on the need to protect sources and informants from being targeted by terrorists. Some of these agreements, such as the ones of the most formalised and best-known intelligence networks between the signals intelligence services of the UK Canada, Australia, New Zealand and the US, have been negotiated by their heads of states.[13] The majority of intelligence sharing, however, is not based on these formal, multilateral agreements, but rather on bilateral network agreements negotiated by the national intelligence agencies themselves, and put down in memoranda of understanding (MoUs), as non-binding, soft law agreements, and

[10] Gerald Staberock, 'Intelligence and Counter-Terrorism', in: Ana Maria Salinas de Frias, Katja LH Samuel, and Nigel D. White (eds.), *Counter-Terrorism; International Law and Practice*, Oxford University Press, 2012, pp. 351-387, at p. 354.
[11] Sepper, *op cit.* p. 155.
[12] Sepper, *op cit.* p. 157.
[13] *Ibid.* See for more information on other multilateral arrangements such as the UKUSA Agreement, the Club of Berne, the Kilowatt Group, the NATO Special Committee, and the Egmont Group of Financial Intelligence Unit, Stéphane Lefebvre, 'The diffuculties and dilemmas of international intelligence cooperation', in: *International Journal of Intelligence and Counterintelligence,* Vol. 16, 2003, pp. 527-542, at 529-532.

without the need for approval by the national legislator.[14] Even less formal arrangements, with an even bigger flexibility and adaptability, are the oral agreements or personal friendships among intelligence agents.[15]

As a result of the self-regulating and secret nature of the transnational intelligence networks, Sepper concludes that there is a significant risk that democracy and human rights are undermined.[16]

3. Human rights framework

Terrorism-related criminal trials have performative power in the sense that the state, through the public prosecutor, sends a message that the threat of terrorism is being dealt with, while concurrently human rights, such as the right to a fair trial, are respected.[17] Yet, because there is an increased reliance on intelligence-led law enforcement,[18] there are general human rights concerns to its admissibility in criminal proceedings, as well as accountability concerns.[19] These apprehensions are, perhaps, most pressing in relation to international cooperation and intelligence sharing across borders. These concerns, moreover, cannot be separated from the other measures that have been adopted by states, and which have triggered a lot of criticism, such as:

- extended maximum limit of pre-charge detentions;
- limited possibility of review of the legality of detention;
- broadening of the scope of evidence that can be withheld from the defence;
- the measures taken that directly impact the presumption of innocence;
- the overly broad use of anonymous witnesses; and
- evidence used as a result of physical or undue psychological pressure, including torture or ill-treatment.[20]

These developments run the risk of undermining the basic principles of rule of law, balance of power between the executive and the adjudicative power and the legitimacy of the democratic state that has an obligation to protect these values. In other words: *Quis custodiet ipsos custodes*? Who guards the guardians?

The rules governing prosecution and trials as well as the international cooperation in criminal matters are clear and in line with fair trial principles. However, no such single standard or homogenous model exists on intelligence oversight and control when exchange of intelligence takes place. On the contrary, the exchange agreements between states are largely confidential. This fact has, in certain circles, contributed to the perception that the intelligence services may be allowed to act in ways prohibited to law enforcement agencies, or that they are somehow otherwise exempt from binding norms of international law. This is of course a false perception. Yet, it poses a risk, as it might inflict a corporate culture in which the framework of human rights are not integrated into the daily activities This can be remedied with human rights training and policy dialogue in order to give some guidance on the basic framework of human rights that is applicable to the use and gathering of intelligence. Also a better communication on the mandates of the intelligence agencies to the outside world might emasculate that perception.

This basic human rights framework is derived from two sets of principles: the general obligation to uphold the principles of human rights in a negative way (to respect and thus not to violate) as well as in a positive way (to

[14] Sepper, *op cit.* p. 158.
[15] *Ibid.*
[16] Sepper, *op cit.* p. 166.
[17] Beatrice de Graaf, *Terrorist on Trial: A Performative* Perspective, ICCT-Paper, 15 March 2011, http://www.icct.nl/download/file/ICCT-de-Graaf-EM-Paper-Terrorism-Trials-as-Theatre.pdf, last visited on 28 August 2012.
[18] Report of the United Nations High Commissioner for Human Rights on the protection of human rights and fundamental freedoms while countering terrorism, UN Doc A/HRC/16/50, 15 December 2010, par. 33.
[19] Quirine Eijkman, *op cit.*.
[20] *Ibid.* par. 31.

ensure respect for those rights).[21] States thus have to provide and enforce an effective civil and criminal law framework to deal with serious human rights violations. This framework moreover needs to enable independent investigations into these violations, as well as a system of effective remedies and reparations for these violations. Any violation of these rights incurs state responsibility. The state is therefore responsible for any internationally wrongful acts of anyone acting on their behalf, including the intelligence services or private actors asked to perform intelligence tasks,[22] and who act, wherever a state exercises effective control or authority.[23] The principle of extra-territorial applicability of human rights obligations is especially important to bear in mind when intelligence operations take place on the territory of another state. The principles of state responsibility moreover place obligations on the state vis-à-vis the assistance it provides to third states in the gathering of intelligence on its own territory, as well as the intelligence it receives from third states that is used for the analysis of its own security situation. As a consequence, any intelligence that is gathered while violating the core principles of human rights and which is shared with other states, should be considered to be unlawful by the receiving state. The receiving state should therefore cooperate to bring such violations to an end.[24] Thus, grave violations of human rights, such as torture, enforced disappearances and arbitrary detention, should place serious constraints on cooperation with states that are known to violate these human rights. Furthermore, the prohibition against torture is absolute and a peremptory norm of international law. States should therefore stay away from any form of aiding or assisting in torture, or recognise such practice as lawful.[25] States that know or ought to know that the

[21] UNGA Resolution 56/83 'Resolution on the Responsibility of States for Internationally Wrongful Acts' (28 January 2002), UN Doc A/RES/56/83 Annex Art. 4 (ILC Articles); See for instance art. 2 (1) of the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, art. 2 of the International Covenant on Civil and Political Rights 1966, para. 7 of the Human Rights Committee General Comment no. 31, 26 May 2005, UN Doc/C/21/Rev.1/Add.13, and Human Rights Committee General Comment No. 20, 3 October 1992.

[22] UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Martin Scheinin, 'Compilation of Good Practices on Legal and Institutional Framework and Measures that Ensure Respect for Human Rights by Intelligence Agencies While Countering Terrorism, Including Oversight (5 May 2010) UN Doc A/HRC/14/46 para. 21 (Good Practices Study); International Committee of the Red Cross (ICRC), 'The Montreux Document on Pertinent International Legal Obligations and Good Practices for States related to Operations of Private Military and Security Companies during Armed Conflicts'.

[23] The principle of extra-territorial application is reflected within the jurisprudence of the International Court of Justice, as well as of universal and regional human rights bodies and courts: International Court of Justice, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territories* (Advisory Opinion), 2004, ICJ Report 136, para. 10; jurisprudence by the UN Human Rights Committee: *Lopez Burgos v Uruguay,* Communication No 52/1979 (29 July 1981), UN Doc CCPR/C/13/D/52/1979; *Lilian Celiberti de Casariego v Uruguay,* Communication No 56/1979 (29 July 1981) UN Doc CCPR/C/13/D/56/1979; 'Concluding Observations of the Human Rights Committee: United States of America' (1995) UN Doc CCPR/C/79/Add. 50 paras 266-304; 'Concluding Observations of the Human Rights Committee: United States of America' (2006) UN Doc CCPR/C/USA/CO/3/Rev. 1 para. 10; 'Concluding Observations of the Human Rights Committee: Israel' (2003) UN Doc CCPR/CO/78/ISR para. 11; 'Concluding Observations of the Human Rights Committee: Israel'(1998) UN Doc CCPR/C/79/Add. 93 para 10; 'Concluding Observations of the Human Rights Committee: Poland' (2004) UN Doc CCPR/ CO/82/POL para. 3: 'Concluding Observations of the Human Rights Committee: Belgium' (2004) UN Doc CCPR/CO/81/BEL Para. 6; On the regional jurisprudence, see for instance: Inter-American Commission on Human Rights (IACHR), 'Request for Precautionary Measures in Favour of Detainees Being Held by the United States at Guantanamo Bay' (12 March 2002) 41 ILM 532; Report of the IACHR on Terrorism and Human Rights (2002) OEA/Ser. L/V/II/116 Doc 5 rev 1; *Coard et al v United States* IACHR Case 10.951, Report No 109/99 (29 September 1999) para 37; *Loizidou v Turkey* (App no 15318/89) (1997) 23 EHRR 513 paras 60-1; *Cyprus v Turkey* (App no 25789/94) (2002) 35 EHRR 30 para 77; *Bankavich and others v Belgium and 16 other contracting States* (App noi 52207/99) (2007) 44 EHRR SE5 para 71.

[24] Arts 16-18 and 40-1 ILC Articles, *op cit.;* Gerald Staberock, *op cit.*.

[25] GA resolution 56/83, annex, International Law Commission Draft Articles on Responsibility of States for Internationally wrongful acts, arts. 4 en 16. Article 16 moreover 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, par. 420. 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; Report of the Special Rapporteur on the Promotion and Protection of Human

intelligence they receive is the fruit of torture, inhumane treatment or arbitrary detention, are creating a demand for such information, and are hence forth complicit in the human rights violations.[26] Thus also the mere presence of intelligence agents of state A during the interrogation of a person by intelligence agents of state B while the person's rights are violated, implies that both states should be held accountable. Practical problem, however, is that not all states act in accordance with this obligation.

In a situation of armed conflict, the framework of international humanitarian law sets the limits for any intelligence operation. However, as the Eminent Jurists Panel in its report noted, there is a risk of over-extending war time rules to situations outside genuine armed conflicts, as well as the risks associated with a 'war paradigm' as a form of national security doctrine under the pretext of a need for more and broader powers for intelligence services.[27] Furthermore, the vast majority of the legal academic community is of the opinion that one cannot speak of a global armed conflict against non-state terrorist groups outside any specific territorial conflicts.[28]

4. Dilemmas of intelligence cooperation and issues of accountability

The previous paragraph showed that the legal framework applicable to the activities of intelligence organisations is straightforward. Difficulties arise when intelligence is used in criminal court cases, and when an exchange of information takes place. The combination of the two, when intelligence from a foreign source is used in criminal court cases, introduces yet additional complicating factors.

Intelligence gathering and criminal investigations are two worlds apart – and for good reasons. They serve different purposes, and thus work according to different standards. Gathering intelligence is predominantly directed towards analysing aspects of possible threats to national security. This involves a lack of transparency, since a substantial part of the activities concerns covert operations and intelligence sources that need to be protected. This is not to say that intelligence gathering is beyond any form of accountability, as was made clear in the previous paragraph. Illegally received intelligence that enables you to prevent victims amongst your population or even big events like a next 9/11 attack, can thus entail questions of accountability.

Criminal investigations, on the other hand, and ultimately prosecutions, need to present evidence to build a criminal case. Rights of fair trial apply, such as the presumption of innocence and the equality of arms in order to review and question evidence upon which arrest, detention or charges rest. Transparency and a public hearing are all part of the framework in which prosecution should take place.[29]

Notwithstanding these different purposes, intelligence is used in court cases. This so-called 'judicialisation of intelligence' confronts courts with a range of legal issues such as disclosure, evidentiary standards and the testimony of intelligence personnel in criminal prosecutions.[30] In many states, special procedures are designed to

---

Rights and Fundamental Freedoms while countering terrorism, Martin Scheinin', 4 February 2009, UN Doc A/HRC/10/3, par. 53.

[26] Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while countering terrorism, Martin Scheinin', 4 February 2009, UN Doc A/HRC/10/3, par. 55; See also Report of the Eminent Jurists Panel on Terrorism, Counter-Terrorism and Human Rights, '
Assessing Damage, Urging Action', ICJ, Geneva, 2009, pp. 81-85.

[27] Report of the Eminent Jurists Panel on Terrorism, Counter-Terrorism and Human Rights, '
Assessing Damage, Urging Action', ICJ, Geneva, 2009; see also Christophe Paulussen, *Testing the Adequacy of the International Legal Framework in Countering Terrorism*: *The War Paradigm,* ICCT-Research paper, 28 August 2012, http://www.icct.nl/download/file/ICCT-Paulussen-Legal-Framework-for-CT-August-2012.pdf, last visited on 28 August, 2012.

[28] *Ibid.,* ICRC, 'International Humanitarian Law and Terrorism: Questions and Answers' (5 May 2004).

[29] See on this topic also Quirine Eijkman and Bibi van Ginkel, 'Compatible or incompatible? Intelligence and Human Rights in Terrorist Trials', ICCT Expert Meeting Report, 2011, http://www.icct.nl/download/file/ICCT-Eijkman-vanGinkel-EM-Paper-Intelligence-in-Court.pdf, last visited on 28 August 2012.

[30] Kent Roach, 'When Secret Intelligence becomes Evidence: Some implications of *Khadr* and *Charkaoui II*', in: *Supreme Court Law Review*, Vol. 47, 2009, PP. 147-208, at 147.

allow the use of intelligence in court cases with the intention of both respecting the specific character of the information which implies that sources and modus operandi are kept secret for (state) security purposes, as well as respecting the fair trial principles. Whether this is successfully done, is debatable.

Out of the four case studies (mentioned above),[31] although all four systems have set up special procedures that try to facilitate the use of intelligence in court cases, they are also all very different in the way and to whom intelligence is introduced in the criminal procedure and the extent to which disclosure is made possible. The Netherlands uses the Act on Shielded Witnesses. France works with a system whereby special investigation judges can access classified documents if they have been given access by the Consultative Commission for National Defence Secret and ask for declassification in order to use the information in a public trial; ultimately all evidence needs to be presented publicly in court, and no sentence can be based on secret evidence. The UK uses a system of Special Advocates appointed by the UK Attorney General when information is withheld from the appellant on national security grounds. The Special Advocate may not however communicate with the appellant once he or she has received the secret information. Finally, Canada, also uses a Special Advocates system. They are appointed by the court to protect the interests of defendants who are subject to a security certificate and, at the same time, to ensure the confidentiality of information which would harm national security or endanger the safety of a person, if information is disclosed. Special Advocates can communicate with the suspect based on a summary. Special Advocates can also negotiate the release of information or agree that the claim of secrecy is warranted.

Without casting a verdict on the compatibility of these procedures with human rights procedures, it does raise the pertinent question: when intelligence comes from a third state, what different regulations with regard to disclosure of information apply? Numerous examples of (complicity of) Western liberal countries' involvement in serious human rights violations have been documented. Indeed, it underscores the conclusion that both Western liberal as well as illiberal regimes are guilty of such practices. Both the former UN Special Rapporteur Martin Scheinin as well as the Rapporteur for the Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe Dick Marty raise concerns about the comprehensive system of extraordinary renditions, prolonged and secret detentions, practices that violate the prohibition against torture or other forms of ill-treatment, and the overwhelming evidence of involvement of democratic law-based states.[32] As was shown in the previous paragraph, the question on the legality of these operations is clear. The main problem lies in the question, how to prove the illegality of the activities when state secrecy arguments are always used to prevent disclosure of evidence. Several criminal proceedings against intelligence agents responsible for criminal acts have been conducted.[33] Some with success, although in many cases the 'security must have precedence over freedom'-concept still dictates the extent to which information is made available for the court. Additionally, some actions for damages were brought to court by victims of unlawful acts.[34] In these cases as well, national secrecy arguments mostly prevailed over the rights and needs of the victims.

It is clear that there are still quite a few accountability challenges to counter-terrorism-related intelligence cooperation. For instance, domestic accountability mechanisms cannot be used to scrutinize the methods of foreign intelligence services or the foreign intelligence that is shared with national services, or at least

[31] Quirine Eijkman and Bibi van Ginkel, *op cit.*.

[32] Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while countering terrorism, Martin Scheinin', 4 February 2009, UN Doc A/HRC/10/3, par. 51; Report of the Rapporteur Dick Marty to the Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe, *Abuse of State Secrecy and national security: obstacles to parliamentary and judicial scrutiny of human rights violations*, Doc. 12714, 16 September 2011.

[33] Report of the Rapporteur Dick Marty to the Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe, *Abuse of State Secrecy and national security: obstacles to parliamentary and judicial scrutiny of human rights violations*, Doc. 12714, 16 September 2011, par. 6-21.

[34] *Ibid.*par. 22-31.

to a limited extent. A further dilemma is accountability for technology, which enables intelligence services to monitor the web or collect intelligence themselves, also outside their own territory. Questions on how to deal with accountability issues for the information that American intelligence officers collect in Pakistan, for instance, fall outside the scope of this paper, but surely complicates accountability issues in general even further.

Furthermore, former Special Rapporteur Martin Scheinin, warns that the 'need to know' principle and the 'third party rule' increase the possibility that many countries become complicit in international crimes.[35] He argues that the lack of incentives to request clarification on the way information is obtained or to ensure that the information they share will not be used in a way that leads to human rights violations, contributes to this unaccountability.[36] States might claim that it is difficult to assess under what conditions information has been gathered. It might even be impossible to get that information from the foreign service, as they might have used private companies to gather the information.[37] This in itself, of course, does not release the state from its legal responsibility for the actions of the private companies, as was argued in the previous paragraph. In many cases the intelligence shared is the result of selection and analysis, and thus not the raw data that is easier to trace back. However, the former Special Rapporteur is concerned that this argument is not only used in relation to the states' convenience, but that this practice is also maintained to make it easier to deny any knowledge or responsibility for breaches of international law committed during the process of intelligence gathering.[38] Or to put it even more bluntly, 'the result of information sharing arrangements is to deny any domestic actor, including the courts, the opportunity to make their own decision about the disclosure of information within a certain policy domain.'[39]

As far as a system of peer accountability within the intelligence community should work to uphold the shared professional ethos, it has failed the real test, since network norms will check the power of network partners only when their own interest or principles are at stake.[40] Moreover, since intelligence cooperation is mostly based on the principle of *quid pro quo*, agencies are incentivised not to jeopardise their relationships. This underlying principle can therefore be detrimental for legitimate intelligence cooperation. What price are we willing to pay for intelligence? Partner intelligence services in less democratic regimes, do not offer intelligence for free, but are likely to ask something in return from their partners. It could thus be the case that intelligence services from democratic countries are asked to spy on the immigrant population or dissident groups from the partner regime residing in the democratic country on its behalf.[41] This is perhaps a direct example of how a state can participate in illegal activities, but there are also more indirect effects. After all, when intelligence agents of democratic states, in the hope of receiving good intelligence, aid authoritarian regimes and abusive human rights practices, democratic states sacrifice their authority to promote rights and accuse states of human rights violations.[42] Finally, the complicity of states with the violations of others creates a demand and a supporting environment of abusive practices.

---

[35] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 'Promotion and Protection of all human rights, civil, political, economic, social and cultural *rights*, including the right to development, UN Doc A/HRC/10/3, 4 February 2009, par. 48.

[36] *Ibid.*

[37] Another dilemma relates to accountability for private companies who collect intelligence. This is becoming increasingly more important. Think about what the Global Intelligence files have revealed about the role of the company Stratfor. Wikileaks (2012), *The Global Intelligence Files,* 9 August 2012, website: http://www.wikileaks.org/gifiles/releasedate/2012-08-09.html, last visited on 28 August 2012.

[38] *Ibid.* par. 56.

[39] Sepper, *op cit.* p. 172, referring to a statement by Alasdair Roberts, in: 'Entangling Alliances: NATO's Security of Information Policy and the Entrenchment of State Secrecy', in: *Cornell International Law Journal,* Vol. 36, 2003, p. 355.

[40] Sepper, *op cit.* p. 174.

[41] *Ibid.* p. 175.

[42] *Ibid.* p. 176.

5. Towards intelligent use of intelligence: some recommendations

Good intelligence is key in preserving our security. No state has the 'Eye of Providence', and therefore cooperation of intelligence services plays a crucial role in assessing the security risks that are of importance to the safety of a nation and its interests abroad. However, this cooperation of intelligence services comes with serious challenges to the legality and the legitimacy of the activities of both partners in the cooperation arrangement. Part of these challenges can be minimised by changes to the domestic system of oversight, as well as the culture within domestic intelligence agencies. With regard to the cooperation arrangements, some recommendations can also be made to face the challenges and the risks of human rights violations and undermining of democratic principles.

To ensure respect for the rule of law with regard to the use of intelligence, three aspects are important and point to a series of remarks and recommendation that are applicable to intelligence gathering in general:[43] 1. ensuring human rights in the intelligence cycle, 2. ensuring effective oversight, and 3. ensuring legal accountability. Also most helpful in this respect, is the Good Practices Study conducted by the former UN Special Rapporteur.[44] The recommendations from these three categories should form the guiding principles of the process of intelligence gathering, analysis and dissemination. From these guiding principles, moreover, some specific policy recommendations dealing with the exchange of intelligence can be derived. Concrete follow-up steps, however, are needed in order to implement these recommendations on an international level or incorporate them in any bilateral agreement on the exchange of intelligence.

Guiding principles for intelligence gathering:

1. **Ensuring human rights in the intelligence cycle:**
    a. A clear legal basis and mandate in respect to counter-terrorism measures is needed; it requires that any interference with the rights of individuals must be in pursuit of a legitimate purpose, and that such rights are safeguarded against abuse by ensuring that they are necessary and proportionate in a democratic society.
    b. Intelligence services should stick to their purpose, and thus limit overlap and confusion with law enforcement and criminal justice organs. They should preferably not perform the functions of law enforcement personnel such as detention, interrogation and arresting people.
    c. If intelligence is used as evidence in a court case, than fair trial principles should be respected, thus the information should be tested, and the limited evidentiary value of intelligence reflected.
    d. Judicial authorisation and independent control should be arranged in a way that it respects the security of intelligence information.

2. **Ensuring effective oversight:**
    a. Since there is no uniform legal definition of 'intelligence accountability', this can nevertheless be interpreted through the prisms of political and or democratic accountability, and the related principle of separation of powers. However, these forms of accountability should be linked to legal accountability. The leading principle should be that no area can be removed from any kind of control.

[43] Gerald Staberock, 'Intelligence and Counter-Terrorism', in: Ana Maria Salinas de Frias, Katja LH Samuel, and Nigel D. White (eds.), *Counter-Terrorism; International Law and Practice*, Oxford University Press, 2012, pp. 351-387.

[44] Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Martin Scheinin, 'Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including their oversight' (Good Practices Study), 17 May 2010, UN Doc A/HRC/14/46.

b. Oversight mechanisms can be a multi-level system, consisting, for example, of both internal and external oversight mechanisms. There is however a danger of fragmentation, with no entity to be able to provide the full picture. With regard to intelligence cooperation, oversight bodies should become more aware of the challenges to human rights and democratic principles.
c. Also important is to ensure that the professional culture of the intelligence and security services respect the rule of law, and are actively engaged on human rights issues. Very valuable is an external system that can receive complaints with adequate whistle blower protection.
d. Oversight mechanisms should at the very least be exercised by one civilian institution with complete independence from the intelligence service and the executive. There should also be a form of proper resourcing.

3. Ensuring legal accountability

a. Apart from the obligation under international law to provide and enforce an effective criminal law framework to redress human rights violations, such as torture or secret detention, and thus to conduct prompt, thorough and independent investigation to bring perpetrators to justice, states should also provide victims of such violations with procedural rights and effective remedies.
b. In practice, however, the record is very poor. The absence of criminal accountability of intelligence agents is matched with the lack of effective civil remedies. What needs to sink in is the notion that state secrecy should not be invoked in ways that have the purpose or effect of preventing the disclosure of crimes under international law or attributing responsibility for serious human rights violations. Secrecy invocation should thus not extinguish the essence of the right to an effective remedy and reparation. They should be seen as evidentiary privileged, but not as a bar to prosecutions or remedies. State secret invocations should moreover be subject to scrutiny to assess their validity.

With these recommendations or guiding principles in mind, some policy recommendations can be made in relation to intelligence cooperation. With regard to cross-border information sharing, there are concerns when foreign states use more permissive frameworks, which could result in a form of information laundering. When this information is moreover connected to illegal practices like secret detentions, and torture, it is important to stress that states have both a passive and active obligation under international law to prevent this from taking place. If states become 'consumers' of torture and implicitly legitimize, and indeed encourage such practices, they are violating international law.

Policy recommendation for intelligent intelligence cooperation:

1. Cooperation arrangements should include professional norms on the prohibition against torture, inhumane treatment, and indefinite and arbitrary detention.
2. States should commit to refrain from using information obtained though illegal activities and this should be translated into their own professional norms, as well as into the cooperation arrangements.
3. Cooperation between national oversight bodies should be enhanced. Examples such as the biannual International Intelligence Review Agencies Conference or the ad hoc meetings of the parliamentary intelligence oversight committees of EU members and candidate countries can/should be followed (Report SR, 2009, para. 50). Also the idea of the Belgian Standing Committee I to set up a permanent knowledge-sharing platform for (parliamentary) review

bodies of intelligence services can/should be followed to share best practices on legislation, jurisprudence and general developments in the field. (Report SR, 2009, para. 50.).

4. Difficulties with regard to effective oversight in matters of intelligence cooperation, for instance due to the 'third party rule', which prohibits the party that receives the intelligence to share with any other party, can be fixed by setting up mandates for oversight bodies to review international intelligence, or the agreements that make the intelligence sharing possible.
5. Cooperation agreements could also be scrutinised by oversight bodies as a matter of preventive safeguard.
6. Reform of national legislation in countries that are party to intelligence cooperation arrangements could be considered in order to create the possibility of oversight by both countries' review bodies.
7. With regard to legal accountability of foreign intelligence, the implementation of the above-mentioned recommendations should facilitate criminal prosecution as well as legal claims of victims in case of violations of human rights without jeopardising the state security.

Bibliography

Concluding Observations of the Human Rights Committee: United States of America' (1995) UN Doc CCPR/C/79/Add. 50.

Concluding Observations of the Human Rights Committee: United States of America (2006) UN Doc CCPR/C/USA/CO/3/Rev. 1.

Concluding Observations of the Human Rights Committee: Israel (2003) UN Doc CCPR/CO/78/ISR.

Concluding Observations of the Human Rights Committee: Israel (1998) UN Doc CCPR/C/79/Add. 93.

Concluding Observations of the Human Rights Committee: Poland (2004) UN Doc CCPR/ CO/82/POL.

Concluding Observations of the Human Rights Committee: Belgium (2004) UN Doc CCPR/CO/81/BEL.

Quirine Eijkman and Bibi van Ginkel, 'Compatible or incompatible? Intelligence and Human Rights in Terrorist Trials', ICCT Expert Meeting Report, 2011, http://www.icct.nl/download/file/ICCT-Eijkman-vanGinkel-EM-Paper-Intelligence-in-Court.pdf, last visited on 28 August 2012.

Quirine Eijkman, *Counter-Terrorism, Technology and Transparency: Reconsidering state accountability?*, ICCT-Paper, 2 February 2012, http://www.icct.nl/download/file/ICCT-de-Graaf-EM-Paper-Terrorism-Trials-as-Theatre.pdf, last visited on 28 August 2012.

Beatrice de Graaf, *Terrorist on Trial: A Performative* Perspective, ICCT-Paper, 15 March 2011, http://www.icct.nl/download/file/ICCT-de-Graaf-EM-Paper-Terrorism-Trials-as-Theatre.pdf, last visited on 28 August 2012.

Geneva Centre for the Democratic Control of the Armed Forces (DCAF), Intelligence Working Group, 'Occasional Papers no.3: Intelligence Practice and Democratic Oversight – a Practitioner's View', July 2003.

Human Rights Committee General Comment no. 31, 26 May 2005, UN Doc/C/21/Rev.1/Add.13.

Human Rights Committee General Comment No. 20, 3 October 1992.

Inter-American Commission on Human Rights (IACHR), 'Request for Precautionary Measures in Favour of Detainees Being Held by the United States at Guantanamo Bay' (12 March 2002) 41 ILM 532.

International Committee of the Red Cross (ICRC), 'The Montreux Document on Pertinent International Legal Obligations and Good Practices for States related to Operations of Private Military and Security Companies during Armed Conflicts', http://www.ohchr.org/Documents/HRBodies/HRCouncil/WGMilitary/Session1/MontreuxDocument.pdf, last visited on 28 August 2012.

International Committee of the Red Cross, 'International Humanitarian Law and Terrorism: Questions and Answers' (5 May 2004), http://www.icrc.org/eng/resources/documents/faq/terrorism-faq-050504.htm, last visited on 28 August 2012.

International Court of Justice, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territories* (Advisory Opinion), 2004, ICJ Report 136.

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.

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.

Stéphane Lefebvre, 'The diffuculties and dilemmas of international intelligence cooperation', in: *International Journal of Intelligence and Counterintelligence,* Vol. 16, 2003, pp. 527-542.

Christophe Paulussen, *Testing the Adequacy of the International Legal Framework in Countering Terrorism: The War Paradigm*, ICCT-Research paper, 28 August 2012, http://www.icct.nl/download/file/ICCT-Paulussen-Legal-Framework-for-CT-August-2012.pdf, last visited on 28 August, 2012.

Report of the Eminent Jurists Panel on Terrorism, Counter-Terrorism and Human Rights, 'Assessing Damage, Urging Action', ICJ, Geneva, 2009.

Report of the IACHR on Terrorism and Human Rights (2002) OEA/Ser. L/V/II/116 Doc 5 rev 1; *Coard et al v United States* IACHR Case 10.951, Report No 109/99 (29 September 1999); *Loizidou v Turkey* (App no 15318/89) (1997) 23 EHRR 513; *Cyprus v Turkey* (App no 25789/94) (2002) 35 EHRR 30; *Bankavich and others v Belgium and 16 other contracting States* (App noi 52207/99) (2007) 44 EHRR SE5.

Report of the Rapporteur Dick Marty to the Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe, *Abuse of State Secrecy and national security: obstacles to parliamentary and judicial scrutiny of human rights violations*, Doc. 12714, 16 September 2011.

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while countering terrorism, Martin Scheinin', 4 February 2009, UN Doc A/HRC/10/3.

Report of the United Nations High Commissioner for Human Rights on the protection of human rights and fundamental freedoms while countering terrorism, UN Doc A/HRC/16/50, 15 December 2010.

Kent Roach, 'When Secret Intelligence becomes Evidence: Some implications of *Khadr* and *Charkaoui II*', in: *Supreme Court Law Review*, Vol. 47, 2009, PP. 147-208.

Elisabeth Sepper, 'Democracy, Human Rights, and Intelligence Sharing', in: *Texas International Law Journal,* Vol. 46, 2010, pp. 151-207.

Gerald Staberock, 'Intelligence and Counter-Terrorism', in: Ana Maria Salinas de Frias, Katja LH Samuel, and Nigel D. White (eds.), *Counter-Terrorism; International Law and Practice*, Oxford University Press, 2012, pp. 351-387.

UN Human Rights Committee: *Lopez Burgos v Uruguay,* Communication No 52/1979 (29 July 1981), UN Doc CCPR/C/13/D/52/1979; *Lilian Celiberti de Casariego v Uruguay,* Communication No 56/1979 (29 July 1981) UN Doc CCPR/C/13/D/56/1979.

UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Martin Scheinin, 'Compilation of Good Practices on Legal and Institutional Framework and Measures that Ensure Respect for Human Rights by Intelligence Agencies While Countering Terrorism, Including Oversight (5 May 2010) UN Doc A/HRC/14/46 (Good Practices Study).