Keeping spies and spooks on the right track: ethics in the post 9/11 intelligence era

den Boer, M.G.W.

published in
Ethics and Security
2010

document version
Publisher's PDF, also known as Version of record

3 Keeping 'Spies & Spooks' on the Right Track: Ethics in the Post 9/11 Intelligence Era

Monica den Boer[1]

'I consider myself a moral person – at least I hope I am. But I lied, cheated, manipulated and deceived every day of my CIA career. I stole foreign countries' secrets whenever I could and undermined unfriendly governments. I induced foreign officials to commit treason against their own countries. I saw and I exploited the dark side of human nature more often than I care to remember. I believed then and still do that all these actions were in the service of a noble cause – but no one could have had the kind of career I did without at least some second thoughts.'
(James M. Olson, Former Chief of CIA Counterintelligence, in *Fair Play*, 2006, p. 13)

Intelligence is a 'distasteful but vital necessity.'
(Dwight D. Eisenhower, Supreme Allied Commander in Europe during World War II)[2]

3.1 Introduction

The role of ethics in intelligence is the core subject of this chapter. Intelligence may be regarded as the discrete and often secret acquisition, processing, analysis and presentation of information by specialised organisations, including government organisations. This information is required by policymakers and executive administrations to protect or promote essential state functions, such as the protection of security, international relations and the management of prime economic and other interests. Intelligence as such can also be defined as a dynamic activity which is handled by a series of actors who collect, process, analyse and exploit information for several security purposes, such as the investigation of terrorism, radicalisation, subversion, industrial espionage and serious organised crime. Starting from the observation that the concept of intelligence is wide ranging, the discussion will focus on intelligence-handling by law enforcement agencies as well as intelligence agencies with internal and external policy

1 Thanks to Emile Kolthoff who commented upon a previous draft, and to the anonymous reviewer for very useful comments. Omissions and mistakes are the sole responsibility of the author.

2 www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/our-first-line-of-defense-presidential-reflections-on-us-intelligence/eisenhower.html.

mandates. It is often presumed that although ethics is an important dimension in intelligence-handling, explanations or accountability concerning the methods by which intelligence is gathered and processed is scarce. However, several countries have an elaborate system for monitoring intelligence agencies.

The value attached to intelligence often depends on the political or economic situation. Generally, it is maintained that the more volatile and ambiguous the international context is, the more relevance intelligence may have in the prediction of strategies and moves by foreign armies, governments, businesses and opposition groups. In history and fiction books, one can find several illustrations of the significance of intelligence for governments in determining their political positions. The treacherous domain of covert or secret intelligence-gathering also inspires novelists. A recent example is the novel *Winter in Madrid* by C.J. Sansom,[3] in which a traumatised former British soldier is sent to Spain to disentangle the complicated political situation in pre-Second World War Spain, which is devastated by civil war and torn apart by several political factions. Another example is the thrilling novel *The Janissary Tree* by Jason Goodwin,[4] where the detective alias eunuch Yashim Togalu seeks to uncover a range of murders in the harems of an Ottoman palace, leading him onto a trail to the Janitsars. This is just an arbitrary selection of the wealth of literature that is inspired by the often murky world of 'spies and spooks'.

Intelligence is expected to promote national and international security. If it fails to do so, its relevance may be played down but particularly the means and methods used for the collection of intelligence – disproportionate and privacy-invasive as they may be – will be subjected to more rigorous scrutiny. The flipside of this argument is that the tolerance of 'amorality' in intelligence processes may increase to prevent or curtail perceived security dangers (Drexel Godfrey, 2006, p. 5). This reasoning boils down to a utilitarian argument which advances teleological or goal-oriented thinking: that, in order to prevent grave harm, intelligence professionals must sometimes 'deceive and harm' in order to accomplish security: 'The boundary for these activities lies in their purpose', says Pfaff (2006, p. 67). In a modern day context, utilitarian thinkers like Bentham and Mill would probably argue that an act that contributes to the maximisation of happiness and security of the greatest number of citizens justifies the measure itself, whether or not it is a harsh one. Apart from the observation that this utilitarian card can be played repeatedly and on the occasion of each and every security incident that is defined as an attempt to undermine national security, there will be no recognition of basic principles such as human rights (Olson, 2006, p. 29).

In the post 9/11 era, the utilitarian argument has often been used by politicians, which has demonstrated that it has become more difficult to draw a clear line, given the

3 Published by Pan MacMillan, 2006.
4 Published by Farra, Straus and Giroux, 2006.

moral issues involved in the proportionality of surveillance measures, collateral damage and civilian casualties (Pfaff, 2006, p. 68). Olson says aptly that in times of fear, Americans, for instance, have been willing to 'tolerate intelligence activities they might otherwise abhor in ordinary times' (2006, p. 39). But if one follows this line of reasoning, citizens will only be willing to accept intrusive or immoral intelligence measures if there is a genuine enemy who represents a great and imminent danger. At the other extreme end of the philosophical continuum, one meets the hard core Machiavelli, who emphasised intelligence collection and secrecy as necessary ingredients of waging war, and who admired states that were successful in using intelligence techniques in order to defeat their adversaries. According to Olson (2006, p. 24), we find in Machiavelli 'an unbridled champion for even the most aggressive of intelligence techniques'.
The consequentialist school, on the other hand, takes into consideration the balance between means and ends; the ethical evaluation depends on the consequences of intelligence-handling processes. If these consequences are regarded as human rights infringements, they may be unacceptable; everything else may fall within the limits of acceptability (Born & Wills, 2007). In the ethics debate, the intelligence world often refers to the Just War theory, restyled as the 'Just Intelligence' theory, which recommends a careful consideration of the target of the intelligence as well as the method by which the intelligence is collected. The 'Just Intelligence theory' advances that there may be situations which justify exceptions to normal ethical standards, and requires a just cause, high chances for success, proportional means, minimisation of damage to innocent individuals, and oversight (Posner, 2003). Walzer, who has been the conceptual mastermind behind this thinking, speaks of 'emergency ethics', arguing that in situations of supreme emergency, even strict rules ought to be set aside.[5]
Finally, there is the deontological 'Kantian' approach which rules that some activities can never be justified, the so-called categorical imperative: no derogation is possible from certain fundamental rights. In Europe, this 'moral absolutism' (Olson, 2006, p. 25) is translated in the form of so-called fundamental (non-derogable) rights. According to the European Convention on Human Rights, no derogation is permitted to the right to life, and no-one is to be subjected to slavery, cruelty, inhuman or degrading treatment (Born & Leigh, 2005, p. 18).
The Kantian, deontological position is not written in stone. As we have seen, tolerance limits for unethical conduct by intelligence professionals have come under severe pressure since the tragic events of 9/11 that unleashed the so-called global war on terrorism. There are certainly no fixed positions about what constitutes morally sound and morally bad intelligence, and it is hard to discern a bottom line in this discussion. Intelligence is booming business, and both the means and methods used to collect it are undergoing rapid change, as well as the organisation of intelligence collection and

5 Discussed by Mertens and Goodwin, 2007, p. 37 and 38.

the governance of oversight. We will seek to illustrate the shifting perspective by drawing from the main findings of inquiries into the international intelligence-exchange on weapons of mass destruction in Iraq (2002-2003). The inquiry reports reveal a range of controversial aspects, ethical challenges and value dilemmas to intelligence professionals, but also another layer, which is the instrumental exploitation of intelligence by political authorities. The chapter ends with a normative section on possible remedies to keep intelligence ethics in good shape, both at the professional as well as at the organisational level.

3.2 'Good' Versus 'Bad' Intelligence

The moral judgement of 'right versus might' has been a *Leitmotiv* within Western political thought since Machiavelli. Taking this to the work floor, the practice of intelligence ethics implies that professionals and their organisations that handle sensitive information form a constant moral reflection on the way in which information is gathered, processed and used (Block, 2008, p. 192). Intelligence officers 'need to address, individually and collectively, the issues of the ethics of their profession'.[6] The shift to large-scale bulk use of surveillance technology has altered the work of many intelligence professionals. No longer are they involved in the physical world of human intelligence collection. In fact, many intelligence professionals may be 'comfortably removed from the manipulation of assets or the direct application of lethal force' (Nolte, 2007). The interval between the intelligence activity and the active undermining or dismantling of a terrorist used to be rather large, but with new technology, which allows simultaneous smart gathering of intelligence with the use of lethal means, the interval has become minimised. These shifts, which are dealt with more elaborately later in this chapter, require an adjustment of ethical reflection on the outcome of intelligence performance (Verweij, Chapter 6).

Intelligence and law enforcement agencies often rely on codes of conduct that allow an assessment to be made of the integrity of instruments and methods. Those codes are however – unlike codes of legal ethics or police ethics – rarely disclosed to the public (Born & Wills, 2007). The capacity of intelligence agencies to be self-critical and reflexive may be limited because 'compared with other public institutions intelligence is insulated from external criticism.' (Herman, 2008, p. 333) Moreover, its 'production processes have no clear yardsticks of efficiency (though close relationships with foreign opposite numbers sometimes provide very useful comparisons). Its organisational culture produces high morale, but with it the danger of collective self-satisfaction; the

6 Nolte, W. (2007). Review of *Just War in the Age of Terror,* J.B. Elshtain. New York: Basic Books, 2003, and Ignatieff, M. (2004). *The Lesser Evil: Political Ethics in the Age of Terror*, Princeton, NJ: Princeton University Press.

feeling of being 'special' is liable to produce the 'not invented here' reactions to ideas from outside' (Herman, 2008, p. 333). In other words, intelligence agencies are aware that they need to be on constant watch in order to avoid slipping into complacency.

The situational logic of everyday decision-making processes, including basic processes such as the wording and selection of information, demand refined reflections of the intelligence professional. Even the legal principles enshrined in intelligence laws may be insufficient to provide a conclusive answer in specific situations. Intelligence professionals often work in the in-between-world, the space beyond the law, where individual discretion is required (Born & Wills, 2007). Hence, there may be a considerable gap between the general codes and the nitty-gritty of intelligence-handling. Despite considerable professional awareness of the importance of integrity (Pekel, 2006), some maintain that intelligence professionals have no theoretical and ethical foundation to guide them through the decision-making process (e.g. Goldman, 2006, p. xiii).

Intelligence may also be qualified as 'bad' when it results from technical flaws in the acquisition, processing and presentation by the special investigation services; by the improper use of acquisition methods; by manipulation of the intelligence product (by the services or by the recipients); or by its lack of substance or erroneous or false content. Hence, the qualification 'bad' is not only normative but in fact also too wide and too ambiguous for the ethics debate. In the context of unethical intelligence practices, there is a general association with misrepresentation, the deliberate leakage of information, manipulation, deception, coercion, politicisation (Johnson & Wirtz, 2006, p. 167f), bribery, theft, political and/or economic disruption, sabotage, torture and lethal force. Though there are standards of ethical conduct, it is often accepted that there may be situations which are exceptional, for instance in the event of an emergency, immediate threat or imminent large-scale threats to citizens (Gates, 2006). Purposefully bad intelligence can have several effects: it may lead to an unnecessary infringement of individual privacy, but ultimately it may also lead to an ill-founded large-scale war. In several instances where there has been a public allegation of 'bad' intelligence, committees or inquiries have been created to reconstruct the truth and to explain to the public whether or not the intelligence was misleading (Lustgarten & Leigh, 1994).

The process of intelligence-gathering has also been subject to several highly politicised inquiries. Notably the performance of the intelligence agencies before and during the invasion of Iraq in March 2003 has been investigated in several countries, particularly those that engaged actively in military support, but also in countries where governments gave political support to the invasion. Crises in the professional capacity of intelligence services, as well as their credibility and legitimacy, may be instrumental in forming strategies to improve them and to further professionalise their processes (see analysis later in this chapter).

3.3 Intelligence Trends after 9/11: Booming Business

Over the past decade, and even before 9/11, powers and mandates to conduct intelligence activities have expanded significantly expansion (Born & Wills, 2007). The mandate of intelligence services has been widened in an incremental fashion (Herman, 2008, p. 113; 349; Jäger & Daum, 2009): there has been a move from foreign policy (military, political, economic) and internal security intelligence (terrorism, subversion) to intelligence that covers the threat of serious and organised crime, narcotics trafficking, arms trafficking and trafficking in human beings (Born & Leigh, 2005, p. 16; Herman, 2008, p. 130; Olson, 2006, p. 9). The nexus between terrorism and organised crime remains the subject of a long-standing academic debate (Ridley, 2008, p. 139).

Nevertheless, the intelligence agenda has gradually widened. Herman (2008, p. 349) maintains that this is not simply due to the ending of the Cold War, but because of a diffusion of security threats (see Chapter 1 on the Shifting Security Paradigm). Russia continued to be regarded as a strategic nuclear power; other security threats which have come to the fore include a range of terrorist threats, weapons of mass destruction, ethno-national and religious conflicts, tribal confrontations, fragile states, conventional arms transfers, the safety of extraterritorial peace missions, and mediation and conflict resolution. It is well known that some terrorist activities, for instance those of the former IRA, were financed partly by extortion and protection rackets. Similarly, as Herman (2008, p. 350; 379) claims, international narcotics trafficking has serious implications for foreign policy, and hence, intelligence activities of law enforcement and internationally oriented intelligence agencies may merge, keeping in mind however that the objectives of organised criminals are considered to be very different from those of terrorist movements (Berdal & Serrano, 2002). Gregory (2008, p. 58) analyses the relationship between police and intelligence agencies regarding serious organised crime, and shows how the British Secret Intelligence Service (SIS) and Government Communications Headquarters (GCHQ) produce intelligence, leading to the observation that 'the intelligence services were helping with attempts to disrupt criminal organisations', as well as providing 'some specialist training in deep-cover surveillance and associated technology ...'

Post 9/11 has also been the era in which intelligence activities proliferated (Born & Wills, 2007). A growing number of agencies has appeared on the scene that handle intelligence in all kinds of domains, varying from public to private, national to international, from open source to secret, and from general to specific (think of the special investigation agencies like Social Intelligence and Investigation Office (SIOD) or the Fiscal Intelligence and Investigation Office (FIOD in the Netherlands). The effect is that intelligence is subject to a vast increase in terms of volume, but at the same time it may lose its particular value and suffer from devaluation due to the open and interconnected environment in which information is gathered and analysed.

Intelligence has always been collected as part of warfare: spies, informers, scout-masters were sent into foreign lands to gather information about vulnerabilities, political opposition, market opportunities (Herman, 2008, p. 9). Secret information has never been clearly separated from other kinds of government information (Herman, 2008; 2010). Government authorities are both the requestors and recipients of sensitive information. With this double role in hand, they are capable of prioritising the focus of intelligence-gathering, and of allocating budgetary resources for specific intelligence purposes. Intelligence is thus closely related to governmental power (Herman, 2008, p. 13).

From the perspective of governments, intelligence as a form of warfare is cheap compared with material expenditure resources like a frigate (Herman, 2008, p. 38). On the other hand, however, intelligence-gathering capacity cannot be isolated from material resources (think of the surveillance capacity of aeroplanes and marine vessels). Moreover, intelligence budgets have increased significantly[7], despite the fact that the Cold War is now well behind us (Johnson & Scheid, 1997; Herman, 2008, p. 347). For countries that have active international stances and relatively high foreign policy presence on the world stage, like the USA, the role of intelligence is still seen as important, given also its close relationship with military power (Herman, 2008, p. 345).

'High policing strategies' (Brodeur, 2007) have become part and parcel of regular police work and have become practices ingrained in 'low policing strategies'. Bayley and Weisburd (2009, p. 82) define high policing as a practice that is highly different from standard practices of normal or low policing 'because it is less transparent, less accountable and less careful with respect to human rights …'; 'In general, high policing encourages a top-down command structure and changes the orientation of police from servicing to controlling the population' (id., p. 82). Not only have law enforcement agencies followed and further elaborated on the transnational networks of state intelligence agencies, 'intelligence' has also become a metaphor for 'smart policing' as well as for law enforcement processes that are guided by information. Many police forces have adopted the model of 'intelligence-led policing' (Den Boer, 2002; Harfield, MacVean, Grieve & Phillips 2008; Ratcliffe, 2002). Intelligence seeks to reduce uncertainty by identifying patterns, and this helps to improve the prediction of crime and disorder which present themselves in a random way (Phillips, 2008, p. 26). Pre-

7 The US non-military intelligence budget totalled $49.8 billion in 2009, marking a $2 billion increase from the previous year. The US government is required by law to reveal its non-military intelligence budget, but the amount spent on military intelligence remains classified. Source: www.thaindian.com/newsportal/world-news/us-non-military-intelligence-budget-totals-nearly-50-bn-in-2009_100268033.html. However, in September 2009, the US Director of National Intelligence, Admiral Dennis Blair, who is responsible for overseeing the 16 USA intelligence agencies with a total of 200,000 employees, was reported as saying that the annual expenditure for the total intelligence programme was 75 billion dollars. In 1994, the annual budget for intelligence activities totalled a 'mere' 24 billion dollars (source: www.intelligencenews.wordpress.com/2009/09/18/01-245/).

vention and anticipation have thus become leading principles of modern day policing. In this line, many police agencies have introduced changes in the era post 9/11, and have developed knowledge and intelligence capacity in areas such as response to weapons of mass destruction and risk assessment (Bayley & Weisburd, 2009, p. 87). As undercover policing or 'special investigation methods' have long since been promoted and used with respect to organised crime and ideological crime (Hirsch Ballin, 2007). Ethical questions thus loom large, as information about undercover or clandestine intelligence activities that may prevent, undermine or interrupt a criminal act, is limited, and may therefore be difficult to control (Bayley & Weisburd, 2009, p. 94). Future research should look at 'the degree of visibility required under law with respect to proactive counterterrorism actions.' (Bayley & Weisburd (2009, p. 85).

Intelligence-led policing increasingly seeks to capitalise on so-called 'community intelligence': information that resides within communities is being considered as a crucial element in the 'signalling' of crime, as well as in the prevention of radicalisation and terrorism. Community intelligence is to be collected by local law enforcement officials from the members of the community, who act as the 'ears and eyes of the community' (MacVean, 2008, p. 70; Bayley & Weisburd, 2009, p. 91); neighbourhood police officers are (technically and formally) capacitated to take this intelligence through the hierarchy to a 'need to know' official (Gray & Slade, 2008, p. 515). Moreover, in an intelligence-led policing model there is a high tolerance of covert activities, such as technical surveillance, the deployment of informants, agents, undercover agents such as infiltrators, pseudo-companies, controlled delivery etcetera, which in many ways is the 'police equivalent of espionage' (Phillips, 2008, p. 30; Parlementaire Enquêtecommissie Opsporingsmethoden, 1996).

The merging or overlap between 'high' and 'low' intelligence activities may have its drawbacks, however. For one, according to Harfield et al. (2008, p. 3),

> *'a situation has been created in which the expectations of "intelligence" in policing are high; there are defined intelligence professionals who do not have control over the use of intelligence but are likely to be singled out for criticism in identified intelligence failings at a time when public confidence in intelligence has been shaken; and a defined structure which includes "intelligence" in its title but is in fact a business model used to direct activity towards achieving performance management targets rather than necessarily responding to the prevailing crime and community safety environment. This context is the domestic policing and community safety equivalent of the "fog of war" that so bedevils military intelligence.'*

With Grieve (2008, p. 22), one could argue that '... intelligence is a system which operates in a non-linear world; there are a vast number of communications, interconnections, and multiple feedback operations.' The challenge to design an effective, efficient and ethical oversight mechanism is thus formidable, given the fluid and heterogeneous character of intelligence and its high-trust environment.

3.4 Governing Intelligence

The institutionalisation of intelligence processes has been a continuous development. Governments organise their intelligence capacity in multifarious ways. Intelligence is generally not in the hands of sole assessors (Herman, 2008, p. 263) and is increasingly handled by agencies other than just secret agencies: think also of other applications, such as ethics and journalism, competitive ethics (in business environments) etc., in view of tackling organised crime, drug-trafficking, extremism and radicalisation. Through enhanced interoperability, joint intelligence data bases and multi-agency co-operation, one may witness eroding walls between the agencies. Hence, counter-terrorism strategies after 9/11 have reinforced the trend of inter-agency and multi-disciplinary intelligence activity (Brodeur, 2007; Haggerty & Ericson, 2000, p. 611; Grieve, 2008, p. 18). Moreover, the post 9/11 era has opened the door further for a blurring of former distinctions between military and non-military intelligence.
In the face of an increased sense of urgency and the need to step up international co-operation, the tendency after 9/11 has been to transform the governance of counter-terrorism efforts. Most visible is the move toward increased centralisation or central co-ordination of intelligence activities (Den Boer, 2002, p. 152; Lander, 2008), particularly in countries with a crowded security policy arena. In the Netherlands, for instance, 20 different organisations are involved in counter-terrorism activities, which has led to the creation of the National Co-ordinator on Terrorism (NCTb), June 2005).[8] In the UK, which has a longstanding history of counter-terrorism efforts, there is no single department that is responsible for the co-ordination of counter-terrorism activities. Like the Netherlands, the UK has a de-concentrated police system, and works using a similar co-ordination model in the format of the National Counter Terrorism Security Office (NaCTSO),[9] which is a police unit that works closely together with security teams. NaCTSO was initiated and is funded by the Association of Chief Police Officers (ACPO), assisting the government with protection and preparation against terrorist activities. One of its tasks is to co-ordinate security advice through a counter-terrorism security advisor (CTSA) and to build relationships between police, government and communities.
Moreover, since 2003, the UK has had a Joint Terrorism Analysis Centre (JTAC), which is the centre for the analysis and assessment of international terrorism. JTAC is

8 Regeling van de Ministers van Justitie en van Binnenlandse Zaken en Koninkrijksrelaties van 29 juni 2005, nr DDS5357209, houdende instelling van de Nationaal Coördinator Terrorismebestrijding (Order from the Ministers of Justice and Home Affairs of 29 June 2005, no. DDS5357209, on the establishment of the National Co-ordinator for Counter-Terrorism (NCTb)). The NCTb is responsible for the analysis of information and intelligence, policy development, and the coordination of preventive counter-terrorism measures. (Website: www.nctb.nl/organisatie/wat_doet_de_NCTb)

9 www.natsco.gov.uk.

based in the intelligence service MI5. It operates as an independent organisation and pulls together representatives from government departments and agencies. The Head of JTAC is responsible to the Director General of the Security Service.[10] After 9/11, Former President Bush first created the White House Office of Homeland Security on October 8, 2001. After legislative amendments, the Department of Homeland Security (DHS) became operational in the course of January 2003, integrating 22 different departmental agencies, including the US Customs and Border Agency, the Federal Emergency Management Agency (FEMA), the US Secret Service and the US Coast Guard.[11] A restructuring exercise took place in 2005 aimed at spurring on operational co-ordination and efficiency, the centralisation and improvement of policy development and co-ordination, as well as the strengthening of intelligence functions and information sharing.

Meanwhile, several administrations saw a need to install an intelligence 'czar', often officially labelled Director of National Intelligence. In the USA, the Director of National Intelligence (DNI)[12] has been functioning as the head of the intelligence community, and bears the responsibility for overseeing and directing the implementation of the National Intelligence Program. The office of the DNI integrates foreign, domestic and military intelligence for the purpose of protecting internal security interests and USA interests abroad. The DNI acts as the principal adviser to the President, the National Security Council, and the Homeland Security Council for intelligence matters related to national security. In a similar fashion, the European Union established the position of the EU Counter-Terrorism Co-ordinator after the train explosions in Madrid in March 2004 which left 200 people killed and more than 1,000 people injured.[13] The EU Counter-Terrorism Co-ordinator works within the EU Council Secretariat and co-ordinates the work of the Council in the area of combating terrorism and keeps an overview of the relevant instruments. The EU Counter-Terrorism Co-ordinator is not responsible for the co-operation between the national intelligence agencies of the Member States. This responsibility resides within the Member States, however, it should be acknowledged that the creation of the EU Joint Situation Centre (SitCen)[14] and the counter-terrorism mandate of Europol[15] imply the bundling and assessment of sensitive intelligence by EU agencies (Ridley, 2008; Van Buuren, 2009; see also Den Boer & Bruggeman Chapter 7).

10 www.mi5.gov.uk/output/joint-terrorism-anlysis-centre.html.

11 For more information, see www.dhs.gov.

12 www.dni.gov.

13 www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/ec/79637.pdf.

14 This agency was set up to monitor foreign and security policy issues, such as weapons of mass destruction and proliferation. Since 1 February 2005, it also has a counter-terrorism remit. Moreover, it collects intelligence which is relevant to EU Missions. SitCen currently comprises over 100 staff members. For an appreciation of the governance of SitCen, see Jelle van Buuren at: www.burojansen.nl/pdf/SitCen2009.pdf.

15 www.europol.europa.eu.

Finally, an illustration of increased centralised governance of intelligence is the creation of national counter-terrorism databases. In 2006, Germany created such a central database, making it possible to quickly locate information within police and intelligence services on persons with connections to terrorism or extremism.[16] This database interlinks several agencies, such as the Federal Criminal Police Office (BKA), the Federal Police Central Bureau (BPOLD), the Land Criminal Police Offices (LKA), the Federal and Land Offices for the Protection of the Constitution (*Bundesverfassungsschutz*), the Military Counter-Intelligence Service (MAD), the Federal Intelligence Service (BND), and the Customs Criminological Office (ZKA). Meanwhile, in the USA, the Terrorist Screening Database (TSDB) has been set up, which is the master terrorist watch list for all federal agencies. The National Counterterrorism Centre (NCTC) is reported to hold the classified reports of the 16 federal intelligence agencies, which some view as the 'mother of all terrorism databases'.[17]

At the same time, in several countries a significant impulse has been given to the 'lateral' organisation of intelligence activity, with the intention to interconnect the intelligence drawn from vertical channels. In tandem with the centralised co-ordination of intelligence activities, and in pursuit of the networked approach, there has also been a lot of 'webbing' of intelligence, particularly through the posting of liaison officers (Bigo, 2000; Block, 2008; Den Boer, 2005; Gill, 2006, p. 28; Grieve, 2008, p. 19; Nadelmann, 1993; Andreas & Nadelmann, 2006). A 'world intelligence structure' has emerged since the onset of the global war against drugs (Grieve, 2008, p. 19). 'Decentralisation' and networked features may be hard to handle by law enforcement agencies who generally work using a vertical organisation of their information-household, but it is generally understood that intelligence is purposefully fragmented and only selected elements of this intelligence find their way to computerised databases (Den Boer, 2002, p. 159). Gill (2006, p. 29) hits the nail right on the head when he argues that the mix of hierarchical-centralised governance of intelligence and the informal-networked governance of intelligence has 'significant implications for oversight'. In addition, Bayley and Weisburd (2009, p. 86) observe that those countries who have cultivated a decentralised counterterrorism structure, require those local or regional police units to undertake counterterrorism operations (e.g. compare the position of the Special Branch in all police county constabularies in the United Kingdom).

Similar tendencies in the direction of lateral intelligence exchange, for instance through counter-terrorism networks and liaison officers, can be seen in international contexts, transnational network structures such as the Police Working Group on Ter-

16 Act on Setting up a Standardised Central Counter-Terrorism Database of Police Authorities and Intelligence Services of the Federal Government and the Länder (Act on Joint Databases) of 2006 (www.en.bmi.bund.de/nn_1016300/Internet/Content/Common/Anlagen/Gesetze/ Antiterrordateigesetz__en,templateId=raw,property=publicationFile.pdf/Antiterrordateigesetz_en.pdf).

17 www.pbs.org/wgbh/pages/frontline/enemywithin/reality/stockton.html.

rorism, the Club de Berne as well as the G6 (Gill, 2006, p. 41; Den Boer, Hillebrand & Noelke, 2008). Herman (2008, p. 350) argues that the international law enforcement intelligence networks such as Interpol and Europol have followed older intelligence: 'its international networks are developing to cope with international crime on the same lines as the intelligence communities' transnational co-operation evolved to meet the threats of Soviet military power and espionage and international terrorism.'
Within the European Union, new policy strategies have been announced with a view to improving the interoperability between the EU databases across the Area of Freedom, Security and Justice,[18] including databases that contain fingerprints of asylum seekers, to customs information, visa records, and data that have been introduced into the Schengen Information System (SIS), which currently contains as many as many as 30 million records Europe-wide (Collett, 2009, p. 46). Originally, the intelligence services had to consult signatory parties to the SIS if they sought access to a so-called Article 99 alert for citizens who are subject to surveillance, but this restriction was removed in 2005 when the EU amended the SIS rules and removed the 'prior consultation requirement' for intelligence agencies (Hayes, 2008). This case illustrates the fact that rules of authorisation and access have been flexed, as well as that the proportionality principle (entry of these alerts only in cases of serious indications) is suffering from erosion. A similar observation applies to the access of security and intelligence services to the EU Visa Information System VIS and the EU Fingerprint System for Asylum Seekers, Eurodac.[19]
The intelligence community has never been homogeneous. The sensitive character of intelligence demands high levels of mutual trust between agencies, but even within the agencies, a deliberate separation between intelligence activities is required. A 'disconnection' or separation of intelligence analysis and those using the intelligence products intends to guarantee the integrity of each of the two processes. 'When these roles become blurred it can distort the line between content and presentation and assessment and advocacy...' (MacVean, 2008, p. 67).[20] Hence, there are two opposing currents: the first one aims at interconnection of intelligence activity across different agencies, the second aims at the opposite, namely preservation of the sharp separation

18 Stockholm Programme after JHA Council meeting 30 November and 1 December 2009, see www.se2009.eu/polopoly_fs/1.26419!menu/standard/file/Klar_Stockholmsprogram.pdf, on p. 39.

19 Opinion of the EU Data Protection Supervisor, Brussels, 7 October 2009. See: www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2009/09-10-07_Access_Eurodac_EN.pdf.

20 According to Olson (2006, p. 246), 'compartmentation is the process of strictly limiting the number of people who are aware of a given intelligence operation. Some writers use the term 'compartmentalization' to describe this principle, but the correct term of art inside the US intelligence community is 'compartmentation'. Only personnel with an absolute 'need to know' should be admitted into the compartment. Simply having the requisite clearance is not enough; the individual in question must have a legitimate work-related reason to know about the operation.'

('firewall') between intelligence and law enforcement agencies. At this point in time, we can only observe a pendulum between these movements.
Accountability for intelligence services is organised according to many different models (Born, Johnson & Leigh, 2005). In most systems, one will find a mixture or combination between parliamentary oversight and executive control. Norms and standards that apply are often derived from universal or international codes, such as the European Convention on Human Rights. Each oversight actor has a different function in evaluating the work of intelligence agencies. Except for matters concerning internal and managerial control, citizens are entitled to submit complaints, media can expose misjudgements or scandals, and interest lobbies are in a position to present alternative views. Formal external control is exercised by the executive, the legislature (i.e. the parliament), the judiciary as well as international organisations (such as the European Court of Human Rights) (Born & Leigh, 2005, p. 15). Oversight authorities hold a key position when it concerns the monitoring of compliance with legal and procedural standards, however, their formal powers can never, by necessity, reach the full scope of intelligence ethics.

3.5 Ethical Challenges in a Changed Intelligence Environment

In an emerging surveillance society which is strongly driven by the desire to control risk, fear and threat, the intelligence services are charged with a special responsibility to guard the interests of citizens as well as equipped with intrusive means of intelligence-gathering. New technology, including DNA-analysis and biometrics, smart cards, RFIDs, and nanotechnology, make it possible for law enforcement and intelligence services to collect data on individuals and to build profiles, which hitherto would only have been gathered if there is an official suspicion. The intelligence environment is changing rapidly, driven by a mutual reinforcement between new technology, which facilitates anticipatory risk-prevention, and flexible legal definitions of terrorism and organised crime.
The first characteristic of the changed intelligence environment is that borders between institutions and databases have become more permeable and can now be transcended (Marx, 1998). Information that used to be inaccessible can now be more easily disclosed, aggregated, analysed and distributed. Information-gathering can be done remotely and anonymously, without the data-subject knowing or realising that a profile is being compiled about him. This may imply that the data-subject remains unaware and that he will not be asked – according to the classic data protection principle – to give his explicit consent. Surveillance and intelligence-gathering will increasingly be performed irrespective of what individual citizens prefer. The absence of a surveillance-contract may slip into a situational void in which a data-subject will no longer be able to exercise his rights. The question of choice, option or alternative for the individual will become paramount in the governance of the surveillance society.

Yet there are several contexts where 'individual choice' is a fiction, as is well illustrated by Marx (1998). The erosion of borders between law enforcement agencies and intelligence agencies falls within this line. The removal of organisational barriers between agencies 'has serious implications for privacy' (Goold, 2007, p. 51).

The second characteristic of this change is that the current 'anxiety society' has become far more focused on the prevention of harm and risk (Aas, 2007, p. 13f; Boutellier, 2002; Ericson, 2007; Zedner, 2007, p. 259f). In this context, intelligence fulfils the role of a precautionary warning system (Herman, 2008, p. 384). Generally, information-gathering has moved from descriptive analysis to predictive analysis: the increased value of predicting the future through threat analysis and risk assessment. This requires intelligence professionals to look beyond the knowledge horizon and to make 'intelligent' appreciations on the basis of scant information; anticipatory intelligence can also lead to decisions supporting pre-emptive wars. According to Herman (2008, p. 34), intelligence is about 'forecasting' and 'prophecy': the output of intelligence in the form of assessments and forecasts is increasingly geared at supporting strategic, tactical and operational performance at all levels of law enforcement activity (id., p. 350). Preventive powers may have a very intrusive effect on people's private lives and are unaccompanied by adequate control, this may lead to problems (Born & Leigh, 2005, p. 16). Closely connected with the use of the precautionary principle is the employment of sensitive (mostly pro-active and undercover) investigation techniques, such using informants (Grieve, 2008, p. 19; Hoogenboom, Chapter 4), which is controversial from an accountability perspective.

The third characteristic is that data volumes are expanding. One could even argue that intelligence-gathering has never been so easy given the potential of new technologies 'to reveal the unseen, unknown, forgotten or withheld' (Marx, 1998). Recently adopted instruments such as the European Union Directive on the Retention of Telecommunication Data and the Passenger Name Records[21] give law enforcement agencies the opportunity to look into vast stocks of private data. With it comes a special responsibility to access to data; authorisation to enter, search or change data; inter-agency exchange of data; verification procedures and so on. Particularly challenging is the 'needle in the haystack' problem where intelligence agencies can be blinded by the huge volumes of data (Adviescommissie Informatiestromen Veiligheid, 2007). Electronic surveillance, data warehousing and data-mining have become part and parcel of ordinary intelligence work.

21 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, pp. 54-63; Communication from the Commission to the Council and the Parliament, 'Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach', Brussels, 16.12.2003 (COM (2003) 826 final).

Issues emerging from these trends include the integrity of information and intelligence. The integrity[22] of intelligence is pivotal: information should not be leaked or sold illegally to interested parties in the full realisation that intelligence can have a transformative effect (e.g. in war situations) (Herman, 2008, p. 147). First, there is the issue of trust and consistency: are all agencies equally reliable and do they operate by the same standards? What about the transfer of the information between agencies? Second: can the intelligence be verified and validated? Are the sources on which the intelligence is based reliable and authentic? Can it be categorically ruled out that the intelligence that has been collected does not rest on coercive interrogation or that it was obtained by torture? Third, by means of which instruments was the intelligence generated? Did the subsidiarity principle prevail, which rules that secret or undercover techniques were used because there were no other means to obtain intelligence? Fourth, what was the consideration of the finality criterion, which lays down the norm that the intelligence is used for the purpose for which it was gathered? Fifth, what are the implications for individuals whose data was gathered and transferred to another agency?

3.6 Intelligence and its Transformative Potential

Governments are the primary consumers of information provided by intelligence services. They base their decisions and policies on this information, making it paramount that the information is accurate and reliable. Hence, the general rule is that intelligence which is provided to a government should not be subject to manipulation or exaggeration to fit institutional or political interests. As we have seen in several inquiries about the intelligence that was gathered on Iraq, there has been ample discussion about the question of who was to be held chiefly responsible the intelligence-gathering process: Did the intelligence services themselves fail to make accurate assessments? Or was it the politicians who used the intelligence to build their case for the invasion in Iraq? Of crucial importance in the 2003 Iraq War was the sharing of information and intelligence with foreign intelligence services. Some information about Iraq was shared in a confidential manner, bilaterally between intelligence services as well as in the multilateral framework of NATO. Countries also share intelligence within frameworks for the export and procurement control regimes like the Australia Group (AG), the Nuclear Suppliers Group (NSG) and the Missile Technology Control Regime (MTCR).

22 The integrity of the intelligence product is a combination of different standards, namely: validity, credibility and 'integre', i.e. obtained in a rightful manner. Within the intelligence and security community 'integrity of information' means that the original format and content have not been changed (and cannot be changed by non-authorised actors).

If intelligence services share information with other intelligence services, they are drawn into a responsibility complex for decisions taken on the basis of this information. Before Iraq was invaded in March 2003 by a military alliance of the US, the UK, Australia, and Poland, and politically supported by a coalition of about 50 countries, several claims were raised by politicians like Colin Powell, and these claims were built on intelligence sources. One building block in the argumentation for going to war was the alleged connection between Saddam Hussein and Islamist fundamentalists (in particular Al Qaeda). One of the hijackers of the aeroplane that flew into the World Trade Center towers on the 11th of September 2001 was Mohammed Atta, who had allegedly been in touch with the Iraqi secret service, the Mukhbarat. These claims were raised in the media around 19 September 2001 and were confirmed by American government sources. There was to be an investigation, but the claims were never substantiated. The then Iraqi Minister of Foreign Affairs, Naji Sabri, and Saddam Hussein wrote an open letter arguing that the American claim about the connection was meant to be a compensation for 'old bills'.[23] Another – retrospective – link between Hussein and Al Qaeda was made about Ibn al-Shaykh al-Libi, a Libyan paramilitary trainer for Al Qaeda who died in a Libyan cell on 10 May 2009; he was interrogated by the American and Egyptian secret services and was said to have claimed (after having been tortured) that there had been connections between Saddam Hussein and the transnational terrorist network of Al Qaeda. It is interesting to note that the claim about the link was not raised often in the public domain by politicians, although initially it was posed as a hypothetical connection.[24]

Another persistent claim at the time was related to a secret informer with the codename 'Curveball', an Iraqi expert on biological weapons, who moved to Germany. He claimed that Iraq had sought to purchase large quantities of uranium ('yellowcake') in Niger; his claims were repeatedly referred to by former President Bush, despite various doubts that had been raised about the credibility and reliability of this informer. Things were getting nasty by September 2004, when the press referred to claims made by Italian diplomats that the yellowcake deal had been fabricated by the French secret service, based on incorrect information from Libya, in an attempt to undermine an American secret service operation.[25]

In a report published by the British government on 24 September 2002, it was claimed that within 45 minutes Iraq could start an attack with chemical and biological weapons. This report, entitled 'Iraq's Weapons of Mass Destruction: an Assessment of the

23 www.nd.nl/artikelen/2001/september/19/kaper-had-contact-met-inlichtingendienst-irak-; www.refdag.nl/oud/vp/010919vp02.html.

24 See e.g. Dutch Prime Minister Balkenende, *Nieuwsbericht*, 9 September 2002.

25 E.g.: *Defense & Foreign Affairs Daily*, July 29, 2003, *Niger-Iraq Uranium Reports Involve Ongoing Libyan Deception Ops.*

British Government',[26] included a foreword by then Prime Minister Blair, saying that 'In recent months, I have been increasingly alarmed by the evidence from inside Iraq that ... Saddam Hussein is continuing to develop WMD, and with them the ability to inflict real damage upon the region, and the stability of the world.' Furthermore, it was stated that 'Intelligence indicates that the Iraqi military are able to deploy chemical or biological weapons within 45 minutes of an order to do so.' Desmond Bowen, head of the Cabinet Office Defence Secretariat, had written a memorandum 13 days prior to the publication of this report to John Scarlett, head of the Joint Intelligence Committee, explaining that he had considerable doubts about the actual threat.[27]

In the years after the Iraq invasion, several questions were raised by members of the Dutch parliament about the intelligence that had been shared between the coalition partners in the framework of NATO, and the assessment of the Dutch government concerning 'material breach' by Saddam Hussein on the basis of intelligence that was made available by its two intelligence and security services. In a response, the Dutch government did not endorse the need to verify which foreign intelligence was used in the Dutch assessment of the threat of WMD.[28] Several questions were raised after the publication of the British Butler Report,[29] which claimed that intelligence about Iraq's attempt to start nuclear and missile programmes had been scarce. The Butler report also concluded that intelligence claims concerning the production of biological weapons in Iraq had not been accurate and that there had been no recent intelligence proving that Iraq had posed a more urgent and greater danger than some other countries which ran WMD programmes. Lord Butler concluded that the British September 2002 report with the 45-minute claim did not take into consideration of the 'thinness' of the intelligence. Moreover, he concluded that there had been no effective application of the normal verification procedures.

What was the situation in 2002 and 2003? The intelligence services were no doubt preoccupied with the global Jihadist struggle and had little capacity to take a critical stance vis-à-vis the intelligence that was produced by partner intelligence services.[30] In addition, partly due to the lack of an explicit mandate, partly because of the dif-

---

26 UK Joint Intelligence Committee, September 2002, www.number10.gov.uk/Page271.

27 13 March 2009, Nigel Morris, 'Secret emails show Iraq dossier was sexed up. Intelligence chiefs criticized 'iffy drafting' of key document.' From: www.independent.co.uk/news/uk/politics/secret-emails-show-iraq-dossier-uwasu-sexed-up-1643960.html.

28 www.minbzk.nl//onderwerpen/veiligheid/algemene/kamerstukken/11895/antwoorden-op_7e; www.minbzk.nl/actueel/kamerstukken/11872/antwoorden-op_86.

29 See e.g questions raised in the Dutch parliament by Van Bommel (SP) and Koenders (PvdA), on 15 and 16 July 2004 respectively (www.minbzk.nl//onderwerpen/veiligheid/algemene/kamerstukken/11872/antwoorden-op_86).

30 Response to parliamentary question about the annual report (2003) of the Dutch Intelligence and Security Agency (AIVD) concerning its foreign intelligence priorities: within the AIVD, there had been a 're-prioritisation' of intelligence-gathering with a focus on fighting Islamist terrorism (www.minbzk.nl//onderwerpen/veiligheid/algemene/kamerstukken/12306/38-vragen-en).

ficulty of running human informers in Iraq itself, human intelligence (HUMINT)[31] about the presence of WMDs or Saddam Hussein's capacity for building a WMD programme had been scant to say the least. Several inquiries on the intelligence assessment concerning the presence of WMD in Iraq have been undertaken since in the US, the UK, Australia, Israel and Germany.[32]

In the UK, several inquiries took place or are still in the process of being undertaken. The Iraq Communications Group (which was an interdepartmental steering group chaired by Alistair Campbell) disclosed a report entitled 'Iraq – Its Infrastructure of Concealment, Deception and Intimidation', which provided information about the resistance that weapons inspectors had encountered in Iraq.[33] The first report after the Iraq war was published on 7 July 2003 by the House of Commons Foreign Affairs Committee about the decision of the UK government to go to war.[34] Many respondents declined the invitation to give evidence to the Committee. It concluded that the intelligence on which the British government had based its decision were not original and mainly depended on information generated by technical means. Then, on 11 September 2003, there was a report (the Taylor Report) from the Intelligence and Security Committee, which is the oversight body of the British secret intelligence services.[35] This committee accepted 'that there was convincing intelligence that Iraq had active chemical, biological and nuclear programmes and the capability to produce chemical and biological weapons.' According to this Committee, Iraq was also continuing to develop ballistic missiles and underscored Iraq's ability to operationalise chemical and biological weapons within 45 minutes. Hence the report backed the British government with the claims it had made on the basis intelligence.

The Hutton Report was published on 28 January 2004 (entitled 'Report of the Inquiry into the Circumstances surrounding the Death of Dr. David Kelly C.M.G.'), on the death of the UN weapons inspector in Iraq and adviser to the British Ministry of Defence. David Kelly had been found dead in July 2003 after it had been revealed that he was the anonymous source of a BBC documentary in which journalist Andrew Gilligan had claimed that the British government had exaggerated the information about

31 This despite the acknowledgement by USA authorities after 9/11 that the weakest link in the collection chain had been 'HUMINT' and that new case officers, assets, analysts, managers and translators were hired with an understanding of the languages and cultures of countries like Afghanistan, Iraq, Pakistan (Johnson & Wirtz, 2004, p. 46; Russell in Johnson & Wirtz, 2004, p.150–151).

32 The Dutch Inquiry into the decision-making process on Iraq published an overview in appendix K, p. 505 (Commissie van Onderzoek Besluitvorming Irak, 2010).

33 The report was discredited afterwards as it had been a compilation of information from undergraduate theses: www.openheidoverirak.nu/?dataint#070703.

34 House of Commons, Foreign Affairs Committee, *The Decision to go to War in Iraq*. Ninth Report of Session 2002-2003, part I, London, the Stationary Office, 7 July 2003; also available at www.parliament.the-stationary-office.co.uk/pa/cmselect/cmfaff/813/813.pdf.

35 Intelligence and Security Committee, *Iraqi Weapons of Mass Destruction – Intelligence and Assessments*, September 2003, www.cabinetoffice.gov.uk/media/cabinetoffice/assets/publications/reports/isc/iwmdia.pdf.

WMD in Iraq and the 45-minute claim. The Hutton Inquiry offered no conclusions about the quality, interpretation and presentation of British intelligence in the pre-war period. The previously mentioned Butler report, which was published on 14 July 2004, was however overtly critical of the intelligence assessments that had been made prior to the war in Iraq.[36] On 15 June 2009, Prime Minister Brown launched an independent inquiry which has to analyse the dossier on Iraq from 2001 to 2009. The findings of the Iraq Inquiry, which is chaired by Sir John Chilcot, are expected in 2011.[37]

In Australia, two parliamentary inquiry reports were published in 2004. The first report was entitled 'Intelligence on Iraq's Weapons of Mass Destruction'.[38] The second report, entitled 'Report of the Inquiry into Australian Intelligence Agencies' (committee Flood), was published on 20 July 2004 and investigated the effectiveness of the Australian intelligence services, their task division and communication.[39] A question which remained unanswered was whether the Australian government had adequately interpreted the information of the intelligence services. The report concluded that the intelligence of the relevant services about Iraq and MWD – in particular the Office of National Assessments (ONA) – was meagre, ambiguous and incomplete, which culminated in the verdict of the Committee Flood that the intelligence work had been an 'intelligence failure of the coalition'.

The Danish Military Intelligence Service (DMIS)[40] was reported[41] as admitting that in a report on Iraq in 2003 it had not been right in concluding that Saddam Hussein had WMD. The assertion was made in a report of the Ministry of Defence to the Danish parliament. The sources on which FE relied at the time were not only limited but also not very reliable. The HUMINT position was difficult and it had been hard to find Iraqis who were prepared to act as informers. Former Danish Prime Minister Rasmussen, who was appointed Secretary General of NATO on 1 August 2009, explained to the Danish parliament that it had not been the intelligence that led to the active military support of the Danes to the Iraq war (submarine and frigate), but the refusal of Saddam Hussein to give his full co-operation the UN WMD inspectors.[42] On 20 April 2004 the DMIS released documents. From a report dating from just before the war (15 March 2003), it appeared that the service had limited information

36 Report of a Committee of Privy Counsellors, Review of Intelligence on Weapons of Mass Destruction, London: The Stationary Office, 14 July 2004 (Butler Report).

37 www.iraqinquiry.org.uk.

38 www.aph.gov.au/house/committee/pjcaad/WMD/report/fullreport.pdf.

39 www.dpmc.gov.au/publications/intelligence_inquiry/docs/intelligence_report.pdf.

40 FE: *Forsvarets Efterretningstjeneste*.

41 *De Morgen*, 4 November 2008: www.demorgen.be/dm/nl/990/Buitenland/article/detail/476623/2008/11/04/Deense-inlichtingendienst-erkent-fouten-in-rapport-Iraakse-WMD-s.dhtml.

42 For the affair with former Major Frank Grevil, who is an expert on WMD, and who served a prison sentence after reporting to the press that he was disconcerted about Rasmussen's exaggeration of the claim that Hussein had WMD, see www.ifex.org/denmark/2006/05/01/two_journalists_indicted_for_reporting/.

about Iraq's operational WMD capacity.[43] The service had claimed in March 2003 that it possessed information that just before the war, Iraq had biological and chemical weapons. Following this affair, the Danish Minister of Defence, Jensby, resigned from his cabinet post on 23 April 2004.[44] Spurred on by the outcome of the Australian inquiry regarding the intelligence failure, the Danish social-democrats demanded a further inquiry towards the end of October 2008 into the DMIS with a specific focus on the evaluation by DMIS of WMD.

The German Foreign Intelligence Service (*Bundesnachrichtendienst* – BND) was claimed to have provided the American CIA with information on a regular basis (15 times) about developments in Iraq.[45] This was particularly controversial as Germany did not provide political support to the invasion of Iraq in 2003. But with the backing of the then German government, the BND had stationed two liaison officers in Baghdad, responsible for identifying non-targets (schools, embassies, hospitals) that should be avoided in a raid. They were allegedly also responsible for identifying so-called high-value targets. The officers were stationed in Iraq between 15 February and 17 March and did not gather intelligence about WMD. There were also allegations of the stationing of a German intelligence officer in Qatar, in the office of General Tommy Franks, US Commander of Operation Iraqi Freedom.[46] The information was given by an anonymous source from within the BND to the ARD. The parliamentary inquiry ended in inconclusive evidence.[47]

France did not support the war in Iraq and the performance of the intelligence services during the war has not been subjected to an official inquiry or evaluation. The *Direction Generale de la Securite Extérieure* (DGSE) did not support the alarming assessments about the presence of WMD in Iraq. A year prior to the State of the Union address by US President Bush in 2003, the French intelligence services were reported to have communicated to the CIA that there was no evidence for the claim that Iraq had WMD. Yet, the chief of the United Nations Monitoring, Verification and Inspection Commission Blix reported to the Dutch Iraq Inquiry committee that Chirac had told him that intelligence services 'had intoxicated one another' (Commissie van Onderzoek Besluitvorming Irak, 2010, p. 285).

In the United States, several inquiries were launched in into the work of the intelligence services. On 9 July 2004 the US Senate Select Committee on Intelligence published a report about Iraqi WMD. Several shortcomings had been identified in the gathering and the analysis of the intelligence. This report was followed by the

43 www.abc.net.au/news/stories/2004/04/20/1090731.htm; news.bbc.co.uk/2/hi/europe/3639977.stm.
44 The Boston Globe, 24 April 2004.
45 According to *Der Spiegel*, 28 January 2006.
46 www.securityaffairs.org.
47 The *Bundestag* Inquiry started on 6 July 2007: www.bundestag.de/bundestag/ausschuesse/ua/1_ua/auftrag/auftrag_erweiter_eng.pdf. The report was published on 18 June 2009 (Bundestag1613400).

Duelfer report on 30 September 2004,[48] reporting the findings of the Iraq Survey Group (ISG) which had been installed by the US Ministry of Defence and the CIA. The ISG was composed of 1,400 American, British and Australian experts on WMD and their security personnel (Duelfer succeeded Kay at the beginning of 2004). The ISG found no proof of the presence of WMD in Iraq. Due to the UN inspections, Iraq had already been forced to terminate its weapons programmes. No proof was found of the existence of missiles either but the ISG found indications that Iraq had the intention to develop and produce long-distance missiles. In September 2006, the US Senate Select Committee on Intelligence published the report 'Postwar Findings about Iraq's WMD and links to terrorism and how they compare with prewar assessments'.[49] This committee was very critical about the accuracy of the findings of the American intelligence services. On 25 May 2007, the same committee published a report entitled 'Prewar Intelligence Assessments about Postwar Iraq'.[50] This focused on the assessment of the consequences of the American invasion by intelligence agencies in the early months of 2003: the report concluded that the intelligence services had reported to the US government that a military intervention would have led to disastrous political, social and economic consequences in Iraq.

Dyzenhaus (2007, p. 148) claims that the reliance placed by governments on the presence of WMD in Iraq as a justification for invasion in Iraq 'has done enormous damage to public confidence not only in the reliability of intelligence information but also in the use to which such information is put by politicians.' A supporter of Walzer's line of thinking ('Just War'; 'Just Intelligence') would argue that a politician is entitled to get his hands dirty when moral and legal rules are broken for reasons of state (Mertens & Goodwin, 2007, p. 38). However, for 'intelligence analysts and managers, politicisation is considered a mortal sin, a fundamental violation of their commitment to provide policymakers with honest answers and estimates.' (Johnson & Wirtz, 2006, p. 167), but at the same time, '… too much analytical detachment or too little interaction between analysts and policymakers, ..., virtually guarantees that finished intelligence will fail to address the issues that fill policymakers' in-boxes' (id., p. 167).[51] The discussion about the politicisation of intelligence about WMD in Iraq (id., 168) evokes the need for a balance between objective and actionable intelligence, as well as a need to identify the ethical dimensions that underlie the appreciation and exploitation of intelligence. Moreover, various inquiries have demonstrated the need for an adaptation of intelligence oversight mechanisms, particularly in view of how intelligence is gathered, how it is validated, to whom it is communicated, by whom it is

48 www.cia.gov/library/reports/general-reports-1/iraq_wmd_2004/index.html.
49 intelligence.senate.gov/phaseiiaccuracy.pdf.
50 Report of the Select Committee on Prewar Intelligence Assessments About Postwar Iraq; intelligence.senate.gov/prewar.pdf.
51 See also Chomeau and Rudolph, 2006.

used, and for what kind of purposes it is used. Particularly in international context, and in order to avoid intelligence agencies 'intoxicating' each other, it is crucial for intelligence agencies to make sure that they avoid information loops and that they produce authentic and verified information. An ethics debate about intelligence could focus on the norm that politicians and governments, who are the principal users of the intelligence, should avoid exploitation and selection of intelligence that best fits their political strategy.

3.7 Ethical Remedies for Intelligence

Intelligence can be a matter of life and death. The accuracy of the intelligence product can thus be regarded as pivotal in the professional handling of information. In this sense, ethics is an essential dimension for any value-based security agency, be it a law enforcement agency or an intelligence service. Thus far, we have discussed the effects of a shifting security climate on security and intelligence agencies that have a mandate to collect intelligence. We have established that there has been a considerable extension of intelligence activity despite the fact that the Cold War is behind us. Partly due to emerging mass surveillance technologies, intelligence activities have been subject to proliferation, culminating in vast amounts of data available to the intelligence agencies as well as leading to a crowded policy arena. This – relatively new – situation gives rise to territorial feuds between intelligence agencies. The competition is paralleled by increased multi-lateral and international intelligence exchange, blurring the original mandates and responsibilities. Moreover, the threshold has been lowered to include 'community intelligence' in preventive strategies against terrorism, radicalisation and extremism.

Intelligence activities have grown in importance, particularly in the business of international police and judicial co-operation. This is the world where one encounters sharp differences between disclosure and data protection rules, as well as a differentiation between the demands for the tuning of ethical principles that underlie intelligence-gathering processes, such as the running of informers and covert human intelligence sources ('CHIPS' in Block, 2008, p. 192f; Hoogenboom, Chapter 4). As intelligence exchange increasingly takes place in international contexts, there is an increased exposure to surroundings that are rife with corruption (Block, 2008, p. 193). In this globalised setting, new intelligence communities emerge that may inhibit a more transboundary and networked character, making it more difficult to discern professional ownership over the intelligence product. Hence, the blurring of intelligence activities may imply serious consequences for ethics and accountability. When translated in research terms, there is a considerable need to map the consequences of this shifting security paradigm for the intelligence domain.

One of the leading questions is whether classical general ethical principles are still upheld by current intelligence agencies. According to Hulnick and Mattausch (2006,

p. 40f), the state must gather information openly if possible, and only use secret methods if necessary; the state should use the least intrusive means of collecting information; intelligence should be presented to politicians and policy-makers without bias or political predisposition; and in order to prevent intelligence from being stolen, states ought to undertake adequate protection measures. Our discussion of the intelligence about Iraq has illustrated that there is a need to contemplate these classic principles again and to build a new culture of corporate reflection inside the intelligence agencies, but also among the principal consumers of the intelligence, namely governments and state services that have a monopoly of violence.

This chapter has argued that ethical principles which are used by intelligence and security services should be made available in the public domain, and that these principles should be made subject to a proper system of internal and external governance, through balanced oversight mechanisms as well as regular training and accountability. A range of professional and cultural organisational measures can be taken, including the encouragement of creativity, critical awareness, and professionalisation. Within intelligence agencies, detailed processes matter a great deal, and they relate to the minute details of drafting, reporting and decision-making on the basis thereof, as well as attention for the various phases and elements of the intelligence cycle (Gray and Slade, 2008). Organisational leadership coupled with professional ethics are regarded as strong and effective variables in the promotion of value-based security organisations; as such, ethical analysis should also be applied by those who conduct the surveillance (Marx, 1998).

An open and reflective culture within intelligence organisations should also welcome an evaluation of 'unethical practices'. In many intelligence surroundings, it is no luxury to promote a new ethics culture. Olson (2006, p. 14), who endorses ethics of intelligence awareness and training reminisces that 'At no time in my CIA career did I receive training in ethics or morality.' Johnson (2006, p. 266ff) advocates an ethics escalation ladder metaphor for weighing the use of specific interventions, such as covert operations, in which the subsidiarity, proportionality, expected effectiveness and intrusiveness are weighed against the importance of undermining the security risks. More emphasis can also be laid on the importance of output legitimacy, or the contribution of the intelligence efforts to making societies safer. As argued above, internal and external oversight mechanisms remain an indispensable lever in the continuous promotion of an ethics-based intelligence culture: 'No profession, particularly one that can hide behind a veil of secrecy, should police itself.' (Olson, 2006, p. ix). In view of the rapid changes in the security landscape, there is a constant need to revisit the quality and authority of oversight mechanisms in national as well as international governance contexts.

References

Aas, K.F. (2007), *Globalization & Crime*. London: Sage.

Adviescommissie Informatiestromen Veiligheid (2007). *Data voor daadkracht. Gegevensbestanden voor veiligheid: observaties en analyse*. Den Haag: Deltahage.

Andreas, P., & Nadelmann, E. (2006). *Policing the Globe. Criminalization and Crime Control in International Relations*. Oxford: Oxford University Press.

Bayley, D.H. & Weisburd D. (2009). Cops and Spooks: the Role of the Police in Counterterrorism. In D. Weisburd, Th. E. Feucht, I. Hikimi, L.F. Mock, and S. Perry (Eds.), *To Protect and To Serve: Policing in an Age of Terrorism*. Dordrecht: Springer.

Berdal, M. & Serrano M. (Eds.). (2002) *Transnational Organized Crime and International Security: Business as Usual*. Boulder: Lynne Rienner Publishers.

Bigo, D. (2000). Liaison officers in Europe: New officers in the European security field. In J. Sheptycki (Ed), *Issues in Transnational Policing*. London: Routledge.

Block, L. (2008). Cross-border Liaison and Intelligence: Practicalities and Issues. In C. Harfield, A. MacVean, J. Grieve, & David Phillips (Eds.), *The Handbook of Intelligent Policing. Consilience, Crime Control, and Community Safety* (pp. 183-194). Oxford: Oxford University Press.

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

Born, H., Johnson, L.K., & Leigh, I. (2005). *Who's Watching the Spies? Establishing Intelligence Service Accountability*. Dulles, VA: Potomac Books.

Born, H., & Wills A. (2007). *Intelligence Ethics: A Complete Cycle?* ECPR conference paper, Pisa. (http://docs.google.com/viewer?a=v&q=cache:uwGFdNAiMcgJ:www.essex.ac.uk/ecpr/events/generalconference/pisa/papers/PP1737.pdf+intelligence+ethics&hl=nl&gl=nl&sig=AHIEtbTy2Dq1xUUfPQT1C6l6CGe1Pk816w).

Boutellier, H. (2002). *De veiligheidsutopie*. Den Haag: Boom Juridische uitgevers.

Brodeur, J.P. (2007). High and Low Policing in Post 9/11 Times. *Policing: A Journal of Policy and Practice*, *1*(1), 25-37.

Chomeau, J.B., & Rudolph A.C. (2006). Intelligence Collection and Analysis: Dilemmas and Decisions. In J. Goldman (Ed.), *Ethics of Spying*: A *Reader for the Intelligence Professional* (pp. 114-125). Lanham: The Scarecrow Press.

Collett, E. (2009). *Beyond Stockholm: overcoming the inconsistencies of immigration policy*, EPC Working Paper No. 32, Brussels: European Policy Centre.

Commissie van Onderzoek Besluitvorming Irak (2010). *Rapport*. Amsterdam: Boom.

Den Boer, M. (2002). Intelligence Exchange and the Control of Organised Crime: From Europeanisation via Centralisation to Dehydration? In J. Apap & M. Anderson (Eds.). *Police and Justice Co-operation and the New European borders* (pp. 151-161). The Hague: Kluwer Law International.

Den Boer, M. (2005). Copweb Europe: Venues, Virtues and Vexations of Transnational Policing. In W. Kaiser & P.Starie (Eds.), *Transnationalism in the European Union. Towards a Common Political Space* (pp. 191-209). London and New York: Routledge.

Den Boer, M., Hillebrand C., & Noelke A. (2008). Legitimacy Under Pressure: The European Web of Counter-Terrorism Networks. *Journal of Common Market Studies*, *46*(1), 101-124.

Drexel Godfrey, J.E. (2006). Ethics and Intelligence. In J. Goldman (Ed.), *Ethics of Spying. A Reader for the Intelligence Professional* (pp. 5-17). Landham, Maryland, Toronto, Oxford: The Scarecrow Press, Inc.

Dyzenhaus, D. (2007). Deference, Security and Human Rights. In B.J. Goold & L. Lazarus (Eds.), *Security and Human Rights* (pp. 125-156). Oxford and Portland, Oregon: Hart Publishing.

Ericson, R.V. (2007). *Crime in an Insecure World*. Cambridge: Polity Press.

Gates, Robert M. (2006) Guarding against Politicization. In J. Goldman (Ed.), *Ethics of Spying*: A *Reader for the Intelligence Professional* (pp. 171-184). Lanham: The Scarecrow Press.

Gill, P. (2006). Not Just Doing the Dots But Crossing the Borders and Bridging the Voids: Constructing Security Networks after 11 September 2001. *Policing and Society*, *16*(1), 27-49.

Goldman, J. (2006). In J. Goldman (Ed.), *Ethics of Spying. A Reader for the Intelligence Professional*. Landham, Maryland, Toronto, Oxford: The Scarecrow Press, Inc., xi-xii.

Goold, B. (2007). Privacy, Identity and Security. In B.J. Goold & L. Lazarus (Eds.), *Security and Human Rights* (pp. 45-71). Oxford and Portland, Oregon: Hart Publishing.

Gray, David and Chris Slade (2008), Applying the Intelligence Cycle Model to Counterterrorism Intelligence for Homeland Security, in *European Journal of Scientific Research*, *24*(4), 498-519.

Gregory, F. (2008). The Police and the Intelligence Services – With Special Reference to the Relationship with MI5. In C. Harfield, A. MacVean, J. Grieve, & D. Phillips (Eds.). (2008) *The Handbook of Intelligent Policing. Consilience, Crime Control, and Community Safety* (pp. 47-61). Oxford: Oxford University Press.

Grieve, J. (2008). Lawfully Audacious: A Reflective Journey. In C. Harfield et al. (Eds.), (2008), *The Handbook of Intelligent Policing. Consilience, Crime Control, and Community Safety* (pp. 13-24). Oxford: Oxford University Press.

Haggerty, K.D., & Ericson R.V. (2000). The Surveillant Assemblage. *British Journal of Sociology*, *51*(4), 605-622.

Harfield, C., MacVean, A. Grieve, J. & Phillips D. (Eds.). (2008) *The Handbook of Intelligent Policing. Consilience, Crime Control, and Community Safety*, Oxford: Oxford University Press.

Hayes, B. (2008). Schengen Information System Article 99 report: 33,541 people registered in SIS for surveillance and checks. *Statewatch*, www.statewatch.org.

Herman, M. (2008). *Intelligence Power in Peace and War*. Cambridge: Cambridge University Press.

Hirsch Ballin, M. F.H. (2007). *Preventing Terrorism through Criminal Law. Using Special Investigative Techniques for the Prevention of Terrorism: A Deliberate Deviation from Existing Thresholds?* Tilburg: Celsus Legal Publishers.

Hulnick, A. S. & Mattausch D.W. (2006). Ethics and Morality in U.S. Secret Intelligence, in Goldman, Jan (2006) (Ed.), *Ethics of Spying. A Reader for the Intelligence Professional* (pp. 39-51). Landham, Maryland, Toronto, Oxford: The Scarecrow Press, Inc..

Jäger, T. & Daum A. (Eds.). (2009). *Geheimdienste in Europa: Transformation, Kooperation und Kontrolle*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Johnson, L.K. & Scheid K.J. (1997). Spending for Spies: Intelligence Budgeting in the Aftermath of the Cold War. *Public Budgeting & Finance*, 17, 7-27.

Johnson, L.K. (2006). Ethics of Covert Operations. In Jan Goldman (Ed.), *Ethics of Spying. A Reader for the Intelligence Professional* (pp. 266-299). Landham, Maryland, Toronto, Oxford: The Scarecrow Press, Inc.

Johnson, L.K. & Wirtz J.J. (Eds.). (2004). *Strategic Intelligence. Windows Into a Secret World*. Los Angeles: Roxbury Publishing Company.

Lander, S. (2008). International intelligence co-operation In A. Christopher, R.J. Aldrich, W.K. Wark (Eds.), *Secret Intelligence. A Reader* (pp. 140-153). London: Routledge

Lustgarten, L. & Leigh I. (1994). *In From the Cold: National Security and Parliamentary Democracy*. Oxford: Clarendon Press.

MacVean, A. (2008). The Governance of Intelligence In C. Harfield, A. MacVean, J. Grieve, & D. Phillips (Eds.), *The Handbook of Intelligent Policing. Consilience, Crime Control, and Community Safety* (pp. 63-73). Oxford: Oxford University Press.

Marx, G.T. (1998). Ethics for The New Surveillance. *The Information Society*, *14*(3), 171-185.

Mertens, T., & Goodwin M. (2007). Democracy and torture: when the people decide In J. Hocking & C. Lewis (Eds.), *Counter-Terrorism and the Post-Democratic State* (pp. 28-47). Cheltenham: Edward Elgar.

Nadelmann, E. (1993). *Cops Across Borders: The Internationalization of U.S. Criminal Law Enforcement*. University Park, PA: Pennsylvania State University Press.

Olson, J.M. (2006). *Fair Play. The Moral Dilemmas of Spying*. Washington D.C.: Potomac Books, Inc.

Parlementaire Enquêtecommissie opsporingen (1996). *Inzake opsporing*. Den Haag: SDU.

Pekel, K. (2006). The Need for Improvement: Integrity, Ethics and the CIA. In J. Goldman (Ed.), *Ethics of Spying*: *A Reader for the Intelligence Professional* (pp. 52-65). Lanham: The Scarecrow Press.

Pfaff, T. (2006). Bungee Jumping off the Moral Highground. Ethics of Espionage in the Modern Age. In J. Goldman (Ed.), *Ethics of Spying. A Reader for the Intelligence Professional* (pp. 66-103). Landham, Maryland, Toronto, Oxford: The Scarecrow Press, Inc.

Phillips, D. (2008). Police Intelligence Systems as a Strategic Response. In C. Harfield, A. MacVean, J. Grieve, & D. Phillips (Eds.), *The Handbook of Intelligent Policing. Consilience, Crime Control, and Community Safety* (pp. 25-35). Oxford: Oxford University Press.

Posner, E. (2003). Do States Have a Moral Obligation to Obey International Law? In *Stanford Law Review*, 51, 1901-1919.

Ratcliffe, J. (2002). Intelligence-Led Policing and the Problems of Turning Rhetoric into Practice. *Policing and Society*, *12*(1), 53-66.

Ridley, N. (2008). Pan-European Law Enforcement Strategic Analysis: Trends and Concerns. In C. Harfield, A. MacVean, J. Grieve, & D. Phillips (Eds.), *The Handbook of Intelligent Policing. Consilience, Crime Control, and Community Safety* (pp. 131-144). Oxford: Oxford University Press .

Van Buuren, J. (2009), *Security as a commodity. Ethical dilemmas of private security*. Brussels: INEX.

Zedner, L. (2007). Seeking Security be Eroding Rights: The Side-Stepping of Due Process. In B.J. Goold & L. Lazarus (Eds.), *Security and Human Rights* (pp. 257-275). Oxford and Portland, Oregon: Hart Publishing.