Revolving doors: ethics in a shifting security paradigm

den Boer, M.G.W.

published in
Ethics and Security
2010

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

1 Revolving Doors: Ethics in a Shifting Security Paradigm

Monica den Boer[1]

1.1 Introduction

Ethics and Security: two entities – or rather discourses – that may have an antagonistic relationship with each other. After a decade in which security threats presented themselves in a fragmentary and transformative fashion, the academic as well as the professional security community is rife with several questions, including the effectiveness and ethics of the instruments that have been designed and introduced to tackle perceived security deficits. With the onset of globalisation, individualisation and computerisation, states have experienced new challenges to their traditional authority and sovereignty. Security, which for the past hundred years has been appropriated and nourished by nation states as a means to control their territory and monitor their citizens, has shifted to arenas that are beyond the control of the state, or hard to access. Privatisation, in the form of the emergence of multi-national security firms, often work with the state but the authority relationship between them is not always clear from the outset. Moreover, security itself has been colonised as a policy, process and product of international organisations and networks, pulling the traditional strings of nation state sovereignty. Ethics – here contextually defined as a composite of norms that underlies value-based security policy[2] – often remain an implicit and obscure dimension. It remains relatively unclear whether ethical values such as integrity, neutrality, independency and equity are addressed in legislation and policy-making, let alone in the minds of security professionals who are responsible for interpreting and implementing security instruments.

This introductory chapter does not seek to be overambitious, as it primarily seeks to map major shifts in the security landscape onto potential ethical questions. Security feeds on discourses about various social tensions that may have a highly disruptive

1 The author would like to thank the anonymous reviewer for useful and relevant comments which have been integrated into the final version of this text. Any omissions remain the sole responsibility of the author.

2 Theoretically oriented discussions about the concept of ethics can be found in other chapters of this volume, e.g., in those by Den Boer, Hoogenboom, Huberts, Kolthoff and Verweij.

potential. Some of these are regarded as deeply ingrained anxieties: xenophobia, populism, unemployment, economic crisis, global warming, and pandemics have willy-nilly become a subject of concern for international organisations, nation states and security organisations. These are very general security dangers that make it hard for security organisations to delineate their responsibility and need for professionalisation. The increased focus on radicalisation, terrorism and organised crime has normalised the employment of proactive and preventive monitoring as regular means to monitor and control deviant behaviour. The rise of a technology-based informational policing places high demands on public and private security organisations and may pushed them beyond the parameters of traditional data protection frameworks.

Four dimensions are fleshed out in which the shifting security paradigm presents itself. The changes in security governance are a first level of analysis. We understand these changes as evolving from, as well as leading to, globalisation, privatisation, pluralisation and hybridisation. These changes are distinct but strongly interrelated patterns of security governance that demand a complete realignment of accountability and ethics standards. However, as we will see throughout the chapter, the complementariness between new governance parameters and accountability mechanisms is underdeveloped in several new security strategies, including those of nation states as well as those that have been created by multilateral entities, such as NATO and the European Union (EU).

The re-framing of the security discourse is based on several sub-developments. For the purpose of this chapter, we have identified and analysed three, namely the wide adoption of anticipatory and risk-assessment based security strategies ('multiple futures'), the wide-spread introduction of prevention and pre-emption in internal as well as external security environments ('precautionary principles'), and the seemingly all-encompassing onset of 'security through surveillance', which profoundly affects the relationship between governing authorities and citizens. The use of the precautionary principle raises several questions about the apparent erosion of the presumption of innocence. Surveillance, which is heavily supported by new technology, raises the normative issue of whether the disappearance of a contractual relationship between the security agent and the object of surveillance ought to be reconfigured.

The chapter concludes by looking at the ethical aspects of emerging security hybrids: those that are characterised by being increasingly multi-disciplinary, by an increase in extra-territorial and cross-border security arrangements, and a blurring of standards between organisations and between what is considered right or wrong (law, politics, media, individual vs institution etc.).

1.2 New Trends in Security

Several authors have dwelled on the issue of security shifts, meaning the notion of security itself, the way it is governed and provided, as well as the guises which security

is adopting (Buzan, Waever & De Wilde, 1998). In a sense, the concept of security is 'liquid' (Zedner, 2006), as well as 'utopian' (Boutellier, 2002). Issues in society which are perceived as problematic, or as hard to control, are likely to become 'securitised' (Aas, 2007, p. 32; Beck, 1992; Huysmans, 2006). Migration, for instance, has been subject to both politicisation and securitisation, particularly in the post 9/11 era, where immigration law has become a centrepiece of anti-terrorism legislation (Aas, 2007, p. 87; Den Boer, 2003, 2008). Throughout the past two decades, the discourse on migration has fundamentally shifted from an inclusive discourse to an exclusionary discourse, culminating in measures of control that are based on a restyling of the immigrant (and asylum-seeker) as deviant or 'bogus' (Den Boer, 1995, 1998). 'Policing' now comprises a whole series of measures including large-scale surveillance, electronic monitoring of borders, the use of biometrics for the purpose of entry and exit, and data-mining enabled by international databases such as the Schengen Information System (SIS). Whilst nation states remain the principal owners, interlocutors and providers of security-related data and network centric environments characterise the intricate global texture in which data is continuously exchanged and analysed across national borders.

When it concerns the notion of security, there is a criminological discourse that advances a cultural thesis about security: the notion of security depends on those who define it. This approach is tolerant of a plurality of definitions. Security – such as crime control – can be a right, to which each citizen is entitled, but it can also be seen as a service or even as a commodity (Aas, 2007, p. 136; Van Buuren, 2009; Van Buuren Chapter 8). Furthermore, there is an influential school of thought that advances the thesis that 'internal and external security are merging' (Aas, 2007, p. 105; Bigo, 2006; Lutterbeck, 2005), or even fusing into one large security amalgam, where organisational and cultural distinctions between the military sector and public police organisations may gradually begin to disappear. At the same time, internal security dangers such as illicit economies, drugs crime and terrorism are increasingly linked with the continuing presence of weak or fragile states. Moreover, there is a growing overlap between internal security issues and foreign policy and external security. This trend is particularly visible in the strategies concerning civil-military security co-operation in the context of EU or UN missions.

The globalisation of security can be regarded as a principal driving force behind the shifting security paradigm. One of the core characteristics in the globalisation of security is the merging of global threats and local fears (Aas, 2007, p. 2; Medcalf, 2008, p. 21). At the same time, 'global' connections that exist on the basis of trade and commerce, internet, migration and travel, rest on a texture which is increasingly characterised by global solidarity and shared vulnerability (Aas, 2007, p. 3). Globalisation marks the growing interconnectedness between states and societies (Held & McGrew, 2007), and 'global flows traverse national boundaries, creating a constant flux between the inside and the outside, resulting in hybridity (sic) of what before appeared to be

relatively stable entities' (Aas, 2007, p. 8). An ontological insecurity (id., p. 15) has become the basis for liquid life, a kind of life in a modern society 'in which the conditions under which its members act change faster than it takes the ways of acting to consolidate into habits and routines' (Bauman, 2005, p. 1).

The privatisation of security is regarded as another essential shift in security. Several authors (Johnston, 1992; Jones & Newburn, 1998; Loader and Walker, 2001, p. 11; Shearing & Stenning, 1987; Cools, 2002; Van Steden & Sarre, 2007; Zedner, 2006, p. 169) have written about this growing multi-national industry in detail. Previously, firms like Securicor, Group 4 Falk A/S and Blackwater acted like commercial chameleons, adopting new names and fusing into new private security amalgams, with the flexibility to cross several security sectors as well as national markets. Some of these transnational private security actors appear 'to bridge the civilian and military sectors, offering to government and corporate clients a range of services including political and security risk analysis, investigations, pre-employment screening, crisis-management and information security' (Gill, 2006, p. 33). For the same reason, information exchange and analysis for security purposes is subject to growing privatisation (Cools, 2002).

In the wake of '9/11', banks, insurance companies and commercial entities furnish public law enforcement agencies and secret services with clients' financial information on their clients which may be privacy-sensitive. Moreover, several multinational companies, such as credit card firms, have their own forensic investigation services, and they conduct their investigations beyond the public realm of supervisory and accountability mechanisms; their flexibility and internationally fluid form of operation means that it is hard to know whether there are any ethical considerations at all, and if there are, to what extent they influence the integrity of investigation practices. Companies that manage the cross-country (i.e. transatlantic) transfer of financial data, such as the Belgium-based company 'Swift'[3], illustrate how globalisation and commercialisation of security are closely entangled. According to Button (2008, p. 11), the liberal democratic view essentially interprets the growth of private security as a consequence of increasing demands on public police, which cannot be satisfied. Despite the overall introduction of New Public Management standards throughout the public law enforcement sector, private security providers are still regarded as more effective providers than their public counterparts (Button, 2008, p. 9). However, the

3 The European Parliament voted to block an agreement by the governments of the 27 Member States of the European Union and the United States to allow personal financial data of European citizens to be analysed by the authorities of the United States that are competent to investigate terrorism. The European Parliament argued that the agreement was not in line with European data protection standards, that the agreement represented a disproportionate invasion of people's private lives; and that it was asymmetric in the sense that the EU does not require private financial data of American citizens to be analysed for counter terrorism investigation purposes. Source: www.europeesparlement.nl/view/nl/press-release/pr-2010/pr-2010-February/pr-2010-Feb-7.html.

regulatory framework for these security companies remains insufficient, at least in the United Kingdom (Button, 2008, p. 95). But in March 2008, the European Parliament adopted common rules[4] for safeguarding aviation, laying down common standards for the screening of passengers and their cabin baggage, but also on the deployment of 'sky marshals' (see also Cools, Davidovic, De Clerck, & De Raedt, 2010).

Even though conditions were imposed on the introduction of these sky marshals, the measure shows how security measures have been introduced via the private sector and raises the question whether public authorities are capable and willing to regulate the standards in the private security sector. The privatisation of security is also prominent in the activity of private military companies (PMCs) and private security companies (PSCs). Several contentious issues emerge from the use of private companies, such as their ambiguous legal status, human rights and accountability issues, and vested interests in conflicts (Schreier & Caparini, 2005). Krahmann (2005) argues that there may be a role for the European Union to tighten control over private military companies, given its mandate in harmonising standards in the free market of goods and services, and given the growing role of the EU in foreign and defence issues (see also White & MacLeod, 2008; Ryngaert, 2008; Cools et al., 2010). One of the questions that comes to mind is whether ethical values in the public sector and the private sector differ a great deal from one another (Van der Wal & Huberts, 2008), which raises the argument that more empirical research ought to be done on ethics in the private security sector, both national and transnational (Van Buuren, 2009).

Meanwhile, several authors are engaged in a modelling of the shifting governance of security. In pursuit of Manual Castells, authors such as Bayley and Shearing (2001), Johnston and Shearing (2003), Shearing and Wood (2007), Gilleir, Easton, Ponsaers, & Cools (2009) have written about the 'nodal governance' of security, which defines the provision of security as concentrating in security bundles provided by a range of authorities. This follows a line of thought where governance – not merely of security, but also of other large-scale issues such as healthcare, education and transport – has become fragmented and pluralised. Hence, the 'pluralisation' of security is one of the main trends that has been identified in security governance (Button, 2008, p. 3): 'Traditional conceptions of the delivery of security have centred around the state as the primary delivery mechanism. However, a growing body of evidence demonstrates that the governance of security has become much more nodal, with 'pluralised' or 'fragmented' modes of delivery' (Button, 2008, p. 5).

4 The European Parliament and Council agreed that Member States are not obliged to introduce sky marshals, however, those Member States that decide to deploy sky marshals "must ensure that they are specially selected and trained". As regards the carriage of weapons, those must not be carried on board an aircraft (with the exception of those carried in the hold), unless the required security conditions in accordance with national laws have been fulfilled and authorisation has been given by the states involved. REF.: 20080307IPR23282. Source: www.europarl.europa.eu/sides/getDoc.do.

The argument put forward by Button is that the police service is increasingly supported by hybrid bodies. Crawford (2006, p. 449) argues that contemporary security governance is not marked by state withdrawal, but by ambitious 'social engineering projects' and 'hyper-innovation' against the background of the 'politicisation of behaviour'. Hence, 'hybridisation' – which operates through hybrid alliances and networks – is regarded as another security shift in the 'post-regulatory state', which is encouraged by the gluing together of security targets and responsibilities. Hybridisation entails that 'no lineage can claim exclusive ownership rights over the product, no kinship group can exercise a pernickety and noxious control over the observance of standards, and no offspring has to feel obliged to swear loyalty to its hereditary lore' (Bauman, 2005, p. 29). When mapped onto hybrid security cultures, this means that there is no overall command of their regulation and accountability, but a plural or diffuse commitment. Hybridisation 'stands for a movement aiming towards a perpetually 'unfixed', indeed 'unfixable', identity' (Bauman, 2005, p. 31).
The commercial character of police and military organisations is an important variable in the convergence between security organisations, leading to a growing overlap between methods, instruments and technologies. This shift is visible in the militarisation of policing and the 'blurring of boundaries' between civil and military organisations. Although the multi-layering, fragmentation, cross-border transcendence and localisation may be visible tendencies, there is still a strong symbolic link between the state and security (Loader & Walker, 2001, p. 24; see also Crawford, 2006, p. 458). Despite the emergence of a 'mixed economy of policing', empirical research demonstrates that private security initiatives are frequently combined with public security investment, which lies in a 'combination of the symbolic power, cultural authority and public legitimacy' of the public security service, 'together with the access to sources of information and intelligence (notably crime-related data) that it facilitates' (Crawford, 2006, p. 463).

Globalisation, privatisation, pluralisation and hybridisation may be closely entangled. All four trends have an impact on the gradual reshaping of the security paradigm and entail a fundamental reorientation on the role of the state in the provision of security: 'Instead of presenting themselves as primarily responsible for addressing the problem of crime, states instead began focusing on making people feel safer and more secure while also arguing that responsibility for such security had to be shared with institutions and organisations outside of the state realm' (Lazarus & Goold, 2007, p. 5).

The emergence of a neo-liberal concept of government means that the state is no longer 'the unquestioned provider or guarantor of public services or certain accepted social rights …' (Lazarus & Goold, 2007, p. 5). Hence, the state has become one player among many, but according to Loader and Walker (2001, p. 11), it remains, or ought to remain, the guarantor of security and policing, based on the monopoly of legitimate

	Globalisation	Privatisation	Pluralisation	Hybridisation
Phenomenon	Provision of security by multi-lateral actors (UN, EU, Organisation for Security and Co-operation in Europe etc), regional entities, non-state actors across the globe	Multi-national, independent, and commercial providers of security	Independent multiple providers of security	Isomorphic providers of security
Context	Institutional and programme-oriented provision of security across a wide range of security issues (ethnic and religious conflict, war-crimes, terrorism, organised crime, illegal migration)	From local to international, e.g. aviation (transport industry), shopping malls, gated communities	International, national and local prevention and repression of crime and public disorder	Post-conflict missions, peace-building activity, para-military crowd control and crisis management
Governance	Public-private co-operation, mostly intergovernmental and hence 'vertical' in style	Regulatory governance, fragmented co-production of security between public and private	Fragmented, networked, de-centralised, horizontal	Multi-lateral, networked, Vertical and Horizontal
Ethics	Widely differentiated environments, standards and implementation unclear, discussion about a 'global constabulary ethic'	Different standards and codes of ethics, but acceptance and implementation not transparent	Differentiated codes of ethics; implementation and oversight unclear	Blurring, tendency to harmonise towards the lowest common denominator, discussion about a 'global constabulary ethic'

Table 1.1 Shifts in Security

coercion, the delivery of civic governance, the guarantee of collective (read equitable) provision of security, and the symbolism of state and nation (see also Crawford, 2006, p. 459). States feed themselves on a perpetual logic of security deficits and crises. This perpetuum mobile nurtures a need for a resourceful and powerful manager. Several authors have observed that the exception becomes the rule, and that states exploit a preventative logic as they themselves have become anxious actors. However, 'values embedded in a pre-emergency institutional culture that take seriously rule of law values is much more difficult to be able to contain official abuses of power, making it more difficult to shift underground' (Ramraj, 2007, p. 200).

1.3 Security Strategies

Recent security strategies have been restyled and focus on the fusion between internal and external security, and promote the interconnection between different approaches. Organisations that deal with security increasingly refer to the so-called 'whole of government' approach or the comprehensive approach, acknowledging the intertwinement between peace and development (Drent & Zandee, 2010, p. 5; Adviesraad Internationale Vraagstukken, 2009, pp. 10, 16; 2010, p. 37).

A document that draws interest is the National Security Strategy of the United Kingdom, carrying the subtitle of 'Security in an Interdependent World' (Cabinet Office, 2008). The main argument in the document is that the international landscape has been transformed: the bipolar power construction in the world has been replaced by a more complex and unpredictable pattern of relationships. Furthermore, it is argued that this implies a considerable shift in the security landscape and that former threats have been replaced by a series of interconnected factors, such as globalisation, climate change, asymmetric distribution of wealth and welfare, competition for energy, as well as demographic shifts (Cabinet Office, 2008, p. 3; Kessler, 2010, p. 17). As a consequence, this 'single overarching strategy' (id., 2008, p. 3) deals with threats emanating from transnational crime, pandemics and flooding, threats that are potentially harmful to large groups of citizens. A crucial shift is the step towards preventive ('early') intervention, even beyond national borders: 'Wherever possible, we will tackle security challenges early. We are committed to improving our ability to scan the horizon for future security risks, and to developing our capabilities for preventive action.' (id., 2008, p. 7). Thus, the document contributes to the gradual codification of pre-emptive action (see below under 'precautionary principles' for further analysis). 'Early engagement' (id., 2008, p. 7) should help to tackle the 'root causes' of terrorism and radicalisation. Across the national borders, this can be done by supporting fragile states and preventing them from further decline. In the spirit of an integrated approach, a multi-lateral and multi-agency strategy is advocated: the police, armed forces, border inspection, intelligence and security services are guided towards building coalitions, together with the private and 'third' sector.

Mimetic language is used in the national security strategy of the Netherlands[5], which acknowledges that several security problems may be caused beyond the national borders. Moreover, it observes the diffusion of security threats and – comparable to the UK strategy – seeks to establish an integrated risk assessment and multi-agency approach. The Dutch strategy document identifies several vital interests, notably territorial, economic, ecological and physical safety, and socio-economic stability. Moreover, it seeks to include a forecasting perspective on the basis of horizon scanning, risk

5 Strategie Nationale Veiligheid, www.minbzk.nl/aspx/download.aspx?file=/contents/pages/87407/.

assessment and scenario-building, while making it coherent with the international security strategies.

In a similar vein, the EU Security Strategy[6], which was adopted in 2003, advocated an integrated strategy with a prominent position for preventive intervention. This entails that the EU seeks to deploy civilian instruments alongside military forces in its approach to conflicts, but struggles with a fragmented authority (Drent & Zandee, 2010, p. 2). The strategy thus promotes a comprehensive approach, particularly by outlining the potential contribution of the EU to crisis management operations (id., 2010, p. 6). The EU Security Strategy views globalisation as a mixed blessing: on the one hand, it encourages free trade and mobility (Cools et al., 2010); on the other hand, it contributes to frustration and injustice. Pandemics, energy, water, food and economic challenges are all seen as issues that are closely interconnected to security. The key threats identified by the EU Security Strategy are: terrorism and violent religious extremism; the proliferation of weapons of mass destruction, including the spread of missile technology; regional conflicts; state failure; and organised crime. The EU concept of a comprehensive security strategy rests on a diffuse threat analysis. Compared with the American perception of security threats, which has lately primarily focused on the threat emanating from global terrorism, the EU promotes a security strategy which 'emphasises the complex causes that lie at the roots of terrorism and locates the causes also within the Union itself' (id., 2010, p. 10).

With the EU, NATO opines that security at home means security abroad (see also Adviesraad Internationale Vraagstukken, 2009, p. 12). In the meantime, NATO has been involved in developing a new Strategic Concept[7] to tackle 'new threats', such as cyber-attacks, piracy, large-scale energy disturbance and fragile states (Adviesraad Internationale Vraagstukken, 2010, pp. 34–35). NATO acknowledges the emergence of a number of 'diverse non-traditional security threats', which challenges the organisation to step beyond its original role. A key characteristic of newly emerging threats is that they no longer have to occur on NATO territory: 'they could affect NATO's security even if they originated from beyond NATO's borders' (Medcalf, 2008, p. 17). But the Strategic Concept 'fails to provide precise answers to the geographic scope of NATO's operations' (id., p. 107). Key sections of the document indicate that the mandate and missions of NATO should not be formulated too precisely; Medcalf

6 Council of the European Union, *A Secure Europe in a Better World. European Security Strategy*. Brussels, 12 December 2003. www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf. See also report on the implementation of the EU Security Strategy: http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/EN/reports/104630.pdf.

7 NATO's 1999 Strategic Concept outlines NATO's fundamental security tasks as security, consultation, deterrence and defence, crisis management and partnership (Medcalfe, 2008, p. 19).

(2008, p. 107) calls this a form of 'constructive ambiguity' – particularly concerning extra-European security challenges – primarily prompted by the events of 11 September 2001.

The common denominator between the European and the American approach is the notion of early defence: nearly a decade ago, the 2002 national Security Strategy of the USA[8] outlined the need to take anticipatory action 'to defend ourselves'. The EU Security Strategy says that 'We need to be able to act before countries around us deteriorate, when signs of proliferation are detected, and before humanitarian emergencies arise. Preventive engagement can avoid more serious problems in the future' (Council of the European Union, 2003, p. 11). The EU employs the discourse of enhancing the security in neighbouring regions and third states, e.g. by using the strategy of Security Sector Reform (Adviesraad Internationale Vraagstukken, 2009, p. 11; Ioannides, 2009, p. 37). Security Sector Reform may however be subject to politicisation, and there may be ethical concerns, particularly at policy implementation levels. Similarly, as Ioannides (2009, p. 39) argues: 'putting military tasks under civilian command, as seems to be the case with the EU SSR mission in Guinea-Bissau, can also have ethical implications on how the EU does peace building.' The EU Security Strategy also proposes that 'common actions' are best based on common appreciations of risk: the sharing of intelligence between Member States and partners of the EU is thus strongly promoted (Council of the European Union, 2003, p. 12).

Also the EU Human Security Report argues that – on the basis of a range of security threats that may undermine citizens and whole communities in their existence – there is a need for a focus on ' human security', in which the referent has shifted, namely from 'state' to 'individual' (Owen, 2010, p. 40). Former Secretary General Kofi Annan launched the concept of human security (Button, 2008, p. 4) and this was developed further by Mary Kaldor who chaired a group of experts and who authored the Human Security report (also known as the Barcelona Report). The human security doctrine advances the thesis that all citizens are equally entitled to live in a secure world, and that this basic right can only be guaranteed when non-military authorities participate in this strategy (Kaldor, 2008). The report argues that the approach to conflicts is best served with a healthy mix of military and civilian capacities. 'Mixed missions' may lead to a blurring of organisational and cultural boundaries between civil and military power (Easton, Den Boer, Janssens, Moelker & Vander Beken, forthcoming), which in itself may cause a reconfiguration of the ethical framework. For instance, the EU endeavoured to establish a Civil Military Cell, which would conduct useful conceptual work for 'hybrid' ESDP missions, 'involving a mix of military and civilian experts ….' (Drent & Zandee, 2010, p. 33). Another illustration of blurred boundaries is the

8 Bush, G.W. *The National Security Strategy of the United States of America,* September 2002, p. 15. Source: www.whitehouse.gov/nsc/nss.html.

development of secure communications, which are regarded as necessary for border control, counter-terrorism and other justice and home affairs activities:

> *'For maritime safety and security civilian authorities need reconnaissance, monitoring and detection capabilities comparable to those in the military inventories. Unmanned Aerial Vehicles can spot illegal immigrants at Europe's external borders using the same sensors which detect irregulars on the ground in deployed military operations in the Middle East or Africa. Airplanes and helicopters are needed for a multitude of civilian-type of activities [sic], including surveillance of critical infrastructure. Improvised explosive devices can pose the same danger in Europe and Afghanistan.' (Drent & Zandee, 2010, p. 67)*

Security research developments within the EU, the European Space Agency (ESA), Space Situational Awareness, Global Monitoring for Environment and Security (GMES) and crisis management operations provide ample material to identify a trend which involves the blurring of organisational, cultural and perhaps ethical boundaries between the internal and external security organisations.
Undercurrents in the shifts in security can thus be summarised as the fusion between internal and external security, an increased focus on extraterritorial engagement, and the gradual acceptance of the early intervention doctrine.

1.4 Multiple Futures

In Europe, and particularly within security agencies such as Europol and Frontex, risk assessment tools have become part and parcel of organisational working methods. These risk assessments and threat analyses, visible in products such as Organised Crime Threat Assessment (OCTA), have evolved into 'strategic future-oriented intelligence systems' (Vander Beken & Verfaillie, 2010). Threat assessments are used as a method to assist policymakers in designing future scenarios of security and policing. Departing from past criminal cases and certain conceptual tools, predictions about serious crime and other security problems are identified (id.): threat analysis, predictive profiling and forecasting are 'based on the assumption that uncertainty can be overcome by developing new information cycles and focuses' (id.).
Risk assessments at the European level build on assessments that are composed at the national level. For instance, the United Kingdom's Serious Organised Crime Agency (SOCA) publishes an annual threat assessment report about various kinds of organised crime, including drug trafficking, fraud, and trafficking in human beings. In a collaborative fashion, the UK Threat Assessment (UKTA) describes and assesses the threats to the UK posed by serious organised crime, to prevent the public and private sector, as well as individual citizens, from falling victim to crime. For instance, the 2006 UKTA specifically addresses the profitability of crime while also addressing the fluidity of criminal networks that make extensive use of 'service providers' and

new information technology.[9] The National Police Agency (KLPD) produces a similar annual threat assessment[10], which emphasises the forecasting perspective, and which will also be fed into the National Intelligence Model (NIM). The national threat assessment is defined as a future-oriented analysis of organised crime in which the threats to Dutch society are addressed specifically. The risk assessment should help to create a base for policy-making and help to prioritise attention for certain crime-development as well as help to focus intelligence-gathering activities. Whilst excluding ideologically motivated crime, such as animal activism, left and right wing extremism, and radicalisation, the Dutch risk assessment report includes all criminal activities that take place in a structured and collaborative manner, as well as those that are aimed at financial profit.

With this wide definition in mind, the risk assessment report covered a wide variety of phenomena, ranging from the trafficking in human beings (exploitation), smuggling of illegal immigrants, illegal trading in and smuggling of weapons and explosives, trading in and smuggling of heroin and cocaine, the production, trading in and smuggling of cannabis and synthetic drugs, the production and distribution of child pornography, the production and distribution of counterfeit money, environmental crime, fraud, money laundering, crime against the property, corruption, use of violence and use of ICT. This was based on a Crime Pattern Analysis (CPA).

An important ethical issue of the forecasting method (Klerks, 2007)[11] in this context is how the information – intelligence – is gathered and whether this involves disproportionate measures at the expense of privacy, but even more pressing is the ethical question concerning the extent to which the forecasting of illegal conduct on the basis of intelligence legitimises law enforcement officers to intervene proactively and to pre-empt malfeasance. Certainly this involves a close reading of the mind of the potential criminal. Early symptoms of future crimes or other forms of misconduct are then subject to social engineering. A closely related ethical question is to what extent it is the duty of the police and judiciary to intervene? Are risk assessments reliable enough to justify early action?

In a similar vein, NATO works by a predictive method and as such it has initiated a multiple futures project, inspired by a growing range of challenges that NATO may currently not be equipped to deal with (NATO Allied Command Transformation, 2008). Opting for a 'spiral approach', the NATO discussion intends to lead to a 'common understanding of key strategic trends, their drivers and a series of possible futures from which the potential challenges facing NATO and implications' could be dis-

9 The United Kingdom Threat Assessment of Serious Organised Crime (2006/7).

10 NTA: National Threat Assessment: www.politie.nl/KLPD/Images/.

11 Klerks quotes S. Bok (1986), *Secrets: on the ethics of concealment and revelation*, Oxford, Oxford University Press.

cussed. In the next section, we will seek to analyse the relationship between risk assessment and the precautionary principle from an ethical perspective.

1.5 Precautionary Principle

The negative and even apocalyptic discourse about insecurity 'provides a justification for 'pro-active' policing, 'pre-emptive' military strikes and 'administrative and exceptional justice', all of which consider anticipated behaviour as sufficient reason for action (Bigo & Guild, 2007, p. 116). According to the same logic, we take 'elaborate precautions against cigarette smoke, obesity, fast food, unprotected sex or exposure to the sun' (Bauman, 2005, p. 69). Kessler (2010, p. 23) regards the precautionary principle as a representation of a 'new discursive practice': 'The shift alters the very relation between the political, the economic and the law and thereby goes beyond the image of a 'broadening' of the security concept' (Kessler, 2010, p. 23), he says, and this newly emerging practice goes along with the anticipatory and calculated management of risk.

In this line of thought, we are moving from a post-crime society to a pre-crime society (Zedner, 2007, p. 259). The pre-crime model has a more 'prospective orientation', which is concerned with the 'calculation of risk and the prevention of future harms in the name of security' (id., p. 259). With Zedner, Borgers and Van Sliedregt (2009) observe the emergence of preventive criminal justice, which increasingly works by the precautionary principle. Their criticism is that the costs of the use of the precautionary principle are not sufficiently taken into account. Against the background of social, legal, economic and political developments, the central notion is that citizens ought to be protected against various dangers. The authors analyse the broadening of criminal liability 'by criminalising the preliminary stage before a harmful act has taken place' (Borgers & Van Sliedregt, 2009, p. 175).[12] In the field of counter-terrorism, the precautionary logic has culminated in 'an expansion of investigatory and prosecutorial power with regard to terrorism' (id., p. 175), which is for instance visible in pre-trial detention. Furthermore, they observe the widening of the use of secret information in court proceedings: notifications from the General Intelligence and Security Service (AIVD) can be used as evidence in criminal cases. Finally, it has been observed that there is now – as a consequence of UN and EU regulations – the possibility to freeze the assets and confiscate possessions of organisations that are suspected of terrorist activities or participation in them. The prevention of crime, through early diagnosis and the active undermining of would-be deviant activity, means that a classic princi-

12 Although the authors sketch this development as being triggered by the post 9/11 response to terrorism, the use of the precautionary principle was already visible in the nineteen eighties, notably in the control of international organised crime and drug trafficking, and codified in, for instance, the Schengen Implementing Convention of 1990 (*Official Journal L 239, 22/09/2000 P. 0019–0062*).

ple of law – namely the presumption of innocence – is left behind, and that the legal system runs a higher risk of imposing wrongful convictions.

But preventive logic is hardly new. According to Zedner, the 'preventive possibilities of policing were recognised even in its origins', but the 'point of intervention has been brought forward' (Zedner, 2007, p. 259), and she associates this with the new – not uncontroversial – doctrine of pre-emption or anticipatory self-defence. 9/11 has given a significant impulse to pre-emptive measures, particularly in relation to radicalisation, terrorism and serious crime (id., p. 260). Actuarial justice, the precautionary principle and the decline of social intervention are also factors that encourage pre-emptive measures and their use.

Indeed, with the onset of the 'War against Drugs' and the later 'War against Terrorism', preventive measures have been widely adopted. Significant is the iterative use of the addendum 'pre', for instance in Dutch criminal law. In her analysis of the prevention of terrorism through criminal law, Hirsch Ballin (2007, p. 13) talks about '*pre*ceding the *pre*-trial investigation a *pre*liminary investigation can take place on the basis of facts and circumstances that indications exist that in a group of people crimes for which *pre*-trial detention can be imposed are being planned or committed.' (my emphasis, MdB). Although the requirement is that these crimes are expected to result in a 'serious infringement of the legal order' and that there should be a reasonable suspicion, the 'public prosecutor can order a preliminary investigation for the purpose of preparing the pre-trial investigation', and as such the preliminary investigation is 'proactive' (id., p. 13).

Despite the fact that preventive and precautionary measures had been introduced widely before 9/11, anti-terrorism legislations introduced since have further lowered standards and thresholds for the use of special investigation methods. For instance, in the Netherlands, terrorism investigation is extended within the preventive phase, and grants 'the public prosecutor without a showing of indications access to stored electronic information upon authorisation of the examining magistrate …'; 'These significant amendments to the law on the use of special investigative techniques are aimed at enabling a system that can effectively confront the immediate and catastrophic threat of terrorism.' (id., p. 67). These developments have been subject to critical scrutiny, as the difference between the work of the prosecution authorities and that of the intelligence agencies is eroding, and come close to governmental infringement of civil rights (id., p. 67), leading to the observation that, at least partially, traditional safeguards of adequate judicial control have been abandoned, or not expanded or improved (id., p. 101). In short, the wide-scale introduction of proactive and preventive investigation methods has not been paralleled by a guarantee of procedural rights.

Similarly, within the external security sphere, the Responsibility to Protect principle (R2P) has gradually gained ground, albeit with controversial discussions concerning the legitimacy of military interventions in foreign jurisdictions. The R2P principle relates both to intervention as well as prevention and reconstruction (Adviesraad Inter-

nationale Vraagstukken, 2009, p. 10). Ban Ki-Moon, the current Secretary General of the United Nations, raised the question of whether sovereignty 'the essential building block of the nation-State era and the United Nations itself, be misused as a shield behind which mass violence could be inflicted on the populations with impunity?'[13] According to Dame Higgins, the term 'Responsibility to Protect' was coined at conference in Canada,[14] where three elements were identified, namely the responsibility to prevent, the responsibility to react and the responsibility to rebuild. The UN doctrine of responsibility to protect also draws criticism, notably from commentators who view the re-articulation of loyalty in distant warfare as falling into line with the old logic of the empire 'despite the sophisticated rationales of human security and the apparent need for humanitarian interventions in many places, …' (Dalby, 2010, p. 55). The discourse which encapsulates the shift in external security is as such coined in the language of geopolitical governance, by taking recourse to the 'vocabularies of imperialism' (id., 2010, p. 57).

1.6 Security through Surveillance

'Surveillance is now so prevalent in modern society that it touches almost every aspect of our daily lives. Our homes, our workplaces and even the public spaces in which we socialize, play and shop, are now brimming with a multitude of sophisticated data collection systems and complex surveillance technologies' (Neyland & Goold, 2009, p. xv). Indeed, technology plays a central role in the surveillance society and in the reconfiguration of security (Barry, 2002). In a globalised world, where states are seemingly losing control, they operate as co-producers of technologically driven security by acting as the sponsors of new technological devices. The financing of new technological developments that are used for the purpose of enhancing security can be seen as an exponent of mobilising power. In the 'techno-industrial complex', where industry, politics and security have developed an intimate relationship, we have witnessed the application of several new technologies in security environments (Cools et al., 2010). Examples include the wide introduction of camera surveillance in public and private spaces; use of fingerprints and biometrics for identity cards such as passports; iris-scans for the pre-boarding procedures; micro-chips that are placed underneath the skin in order to be scanned prior to entry into discotheques; the introduction of infra-red and micro-wave body scanners, particularly at airports; the use of the Global Positioning System (GPS) for the monitoring of mobile telephones; the use of the automatic number plate registration (ANPR) on motorways; the electronic intercep-

13 From A/63/677, 12 January 2009, Implementing the Responsibility to Protect, quoted by Dame Rosalyn Higgins DBE QC, 'Ethics and International Law', Cleveringa Lecture 2009, *mimeo*.

14 Report of the International Commission on Intervention and State Sovereignty, *The Responsibility to Protect*, Ottawa, International Development Research Centre, 2001.

tion of telephone, e-mail and sms-traffic; and the use of radio frequency identifiers (RFIDs) in consumer products.

For instance, the United Kingdom is in the process of constructing an intelligence-based, electronically monitored system of border controls (Cabinet Office, 2008, p. 57), which is ready to be rolled out to the rest of the European Union: 'By 2011, 95% of those entering or leaving the country, whether British or foreign, will be electronically checked against watch lists for terrorism, crime and illegal immigration, as well as being counted in and out of the country; 100% coverage will be completed by 2014.' (id., p. 57). The UK National Security Strategy of 2008 announced that for 'foreign nationals' (apparently irrespective of whether they are from another EU Member State) compulsory fingerprint biometric identity cards would be introduced from late 2008, and in the second half of 2009, identity cards would be introduced for people who work on sensitive locations such as airports.

'New technologies', which are used against potential suspects but also to monitor the wider population, are means which 'no longer see the body as something that needs to be trained and disciplined, but rather as a source of unprecedented accuracy and precision' (Aas, 2006, p. 143). When one sees this observation in a dynamic governance context, in which public and private actors use technology for the purpose of expanding security control, the issue does is not what kind of technology is developed, but by which actor it is used and for what purpose. Technological or electronic surveillance can be compared to a perlocutionary speech act where the effect of a particular technological device gives the surveillance agent the impression that he or she can discipline the object of that security (the [suspected or mobile] citizen), and that the object of the screening or surveillance is made to believe that (s)he contributes to security. Hence, it is not the technology that performs the control, but the actor (e.g. local government authority) that exploits that technology for the purpose of security governance. His or her remote interaction with the object of security is no longer based on an explicit contract but on an expectation that there is a mutual understanding about the necessity and proportionality of the surveillance measure (Den Boer & Van Buuren, forthcoming).

What kind of ethical challenges are implied by the onset of security governance through technical surveillance? Except for impending data protection and privacy issues, there is first of all a change in the interface between the inspector (controller) and the inspected (controlled). The person who is subject to control, whether it concerns a body scan or an electronic interception, puts a tremendous amount of trust the in hands of the person who performs the security or entrance check. This requires considerable reliance on the professional capacity and ethical awareness of the individual in charge. Second, the growing technological interface in security governance implies a considerable reduction in direct human contact, which means that the professional intelligence and knowledge increasingly hinges on data-machines and technology. The growing popularity of 'digicops', policing on the Internet, undercover digital presence

and digital agent provocateurship calls into question whether the same ethical norms apply when the monopoly of violence is held in the virtual world.
Moreover, 'dataveillance' implies the move from the policing of territory to the policing of suspect populations, pushing back the local beat: 'information technologies are in several ways changing the deeply embedded assumptions of police practice' (Aas, 2007, p. 164). There is little reflection on the declining possibility for the subject and object of surveillance to enter into a teleological discussion about whether the surveillance measure is proportionate and legitimate in view of the security objective. In this context, one should note that the agent of security surveillance remains anonymous to the object of that security; the object of the surveillance measure is cannot exercise any form of personal sovereignty or choice, let alone consent. The non-co-operation principle or the right to silence do not apply in these contexts, thereby severely restricting the possibilities for individuals to avoid being seen, monitored, inspected or controlled.
The wider ethical debate is concerned with the question of whether the accumulation of technology-driven security devices brings about a 'Big Brother' society and reassertion of state control (Haggerty & Ericson, 2000, p. 605). The creeping emergence of surveillance measures, 'function creep' (Brown, 2009, p. 63), as well as its vast expansion (Haggerty, 2009, p. 161), mostly authorised by means of administrative measures (Sackers, 2010), implies an 'exponential multiplication of visibility on our city streets' (Haggerty & Ericson, 2000, p. 605).

1.7 Ethical Challenges Evolving from Security Shifts

The emergence of new security threats and the wide propagation of the integrated, preventive, proactive, intelligence-based approach have thus far evoked surprisingly little discussion on ethical ramifications for the security profession and the restyling of public and private security organisations. We conclude this chapter with an indicative itinerary of ethical concerns. A first concern which emerges is whether equity – a norm which implies that all citizens should profit equally from the benefits of a social welfare state as the prime provider of security – can still be upheld in an era of asymmetric distribution of rights, justice, and security and surveillance. Though rich elites are now equally victims of rigorous monitoring of their private habits and commercial transactions, selected groups (the 'dangerous classes') are subject to closer surveillance, to the extent that they are more readily classified as composed images of risk. Their anticipated future deviance is increasingly countered through a series of preventive measures. In short, social engineering has adopted a patriarchal style (compare the use of Anti-Aggressive Social Behavioural Orders in the United Kingdom) through which the behaviour of the masses is anticipated and calculated with the help of surveillance measures. Though proactive intervention in personal lives seems to have become a widely accepted means, it may gradually lead to the erosion of the presumption of innocence. Meanwhile, though the rapid expansion of the private security industry

(Button, 2008, p. 114) may be stopped in its tracks due to the scarcity of economic and financial resources, the asymmetric distribution of security commodities may reinforce an already present pattern of security inequity (id., p. 118).

One of the distinctive characteristics of the new security paradigm is the creation of a security amalgam that fuses internal and external security, and that has the power to blur previously well-guarded borders between police, military and intelligence services. The blurring between police and military, public and private requires new non-horizontal and pluralistic accountability mechanisms in which ethics establish a fundamental cornerstone. Moreover, the blurring of standards may lead to ethical fluidity, but also to a settlement for the lowest common denominator, ethically speaking. The question is why this should be the case, given the salience of good governance norms through accountability and integrity and ethics, both within governmental environments as well as in external security governance (Security Sector Reform, human rights policing, police reform programmes, etc). Yet, if the horizon of our security concerns is subject to constant change, and if this entails the reconfiguration of security organisations and their mandates, an objective and balanced discussion about ethical consequences may be difficult to achieve. Moreover, a performance driven environment will have a tendency to look primarily at effectiveness and only in second instance – or at an ad hoc basis – at ethics.

When we take the accountability and ethics aspects into account, an important factor that comes to mind is that of training demands, which are considerably lower than those of public security professionals (Button, 2008, p. 79 ff). Considering the wide variety of powers which are exercised by private security officers (e.g. denying persons entry to premises, guarding of prisoners), and their engagement with the public, a debate about ethical values appears to be most pressing, and this applies even more urgently in contexts where officials of private security companies function as armed guards with a license to kill. As we have seen in this chapter, this concern applies equally to the private military sector. The observation, shared by several authors, underlines the need for further empirical research into the similarities and differences between ethical values in the public and private sector.

While the discourse on ethics always has been and always will reflect a wide range of opinions, the role of ethics in security has become even less defined due to shifting security lines. Governments may have to reconsider traditional anchors of accountability and supervision of security organisations that are increasingly endowed with intrusive, technologically advanced means. Security professionals may face moral dilemmas in view of their increased competences to monitor and control citizens. Technology designers may have ethical considerations about the potential impact of the surveillance measures they invent.

In sum, with the vastly increased security potential, professionals – like state authorities – may be in need of new anchors in the face of newly emerging ethical dilemmas. In this chapter, we have shown that security ethics is more difficult to define due to

the fact that its discourse is embedded in a complex international governance context. Accountability, ethics and human rights may be taken less seriously in a hardening security climate, which is primarily geared at effectiveness and efficiency (NPM, performance measurement). Another issue to contemplate is whether ethics may start being regarded as a 'soft' issue within a hard management environment. Finally, the complexity of the security ethics discourse increases due to the diversification of security governance relationships: the intricacy of policing and security requires a complementary 'smart', layered and heterogeneous accountability regime. These are tough and urgent questions for governments and citizens alike.

References

Aas, K.F. (2006). The body does not lie: Identity, risk and trust in technoculture. *Crime, Media, Culture*, *2*(2), 143-158.

Aas, K.F. (2007). *Globalisation & Crime*. Los Angeles/London/New Delhi/Singapore: Sage.

Adviesraad Internationale Vraagstukken (2009). *Crisisbeheersingsoperaties in fragiele staten. De noodzaak van een samenhangende aanpak*. The Hague, No. 64 (available from www.aiv-advies.nl).

Adviesraad Internationale Vraagstukken (2010). *Het nieuwe strategisch concept van de NAVO*. The Hague, No. 67, (available from www.aiv-advies.nl).

Barry, A. (2002). *Political machines; Governing a technological society*. London and New York: Athlone Press.

Bauman, Z. (2005). *Liquid Life*. Cambridge: Polity Press.

Bayley, D.H., & Shearing, C.D. (2001). *The new structure of policing; Description, conceptualization, and research agenda.* National institute of Justice, Washington D.C.: Department of Justice. Report 187083.

Beck, U. (1992). *Risk Society. Towards a New Modernity*. London: Sage Publications.

Bigo, D. (2006). Internal and external aspects of security. *European Security*, *15*(4), 385-404.

Bigo, D., & Guild, E. (2007). The worst-case scenario and the man on the Clapham omnibus. In B.J. Goold & L. Lazarus (Eds.), *Security and Human Rights* (pp. 99-121). Oxford and Portland, Oregon: Hart Publishing.

Borgers, M., & Sliedregt, E. van (2009). The meaning of the precautionary principle for the assessment of criminal measures in the fight against terrorism. *Erasmus Law Review*, *2*(2), 171-195.

Brown, I. (2009). Regulation of converged communications surveillance. In B.J. Goold & D. Neyland (Eds.), *New Directions in Surveillance and Privacy* (pp. 39-73). Devon: Willan Publishing.

Button, M. (2008). *Doing security. Critical reflections and an agenda for change*. Basingstoke: Palgrave/MacMillan.

Buzan, B., Wæver, O., & De Wilde, J. (1998). *Security: A new framework for analysis*. London: Lynne Riener.

Boutellier, H. (2002). *De veiligheidsutopie. Hedendaags onbehagen en verlangen rond misdaad en straf.* The Hague: Boom Juridische uitgevers.

Cabinet Office (2008). *The national security strategy of the United Kingdom. Security in an interdependent world*, Presented to Parliament by the Prime Minister, by command of Her Majesty, Cm 7291. London: The Stationary Office.

Castells, M. (2000). *The rise of the network society*. Oxford: Blackwell.

Cools, M. (2002). Onderstromen in de private veiligheidszorg. *Panopticon*, *23*(2), 134-155.

Cools, M., Davidovic, D., De Clerck, H., & De Raedt, E. (2010). The international private security industry as part of the European Union security framework: A critical assessment of the French EU Presidency White Paper. In M. Cools, B. De Ruyver, M. Easton, L. Pauwels et al. (Eds.), *EU and international crime control. Topical issues,* Governance of Security Research Paper Series (pp. 123-136). Antwerp: Maklu.

Council of the European Union (2003). *A secure Europe in a better world – the European Security Strategy*, Brussels, 12 December 2003 (www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf).

Crawford, A. (2006). Networked governance and the post-regulatory state? Steering, rowing and anchoring the provision of policing and security. *Theoretical Criminology*, *10*(4), 449-479.

Dalby, S. (2010). Critical geopolitics and security. In P. Burgess (Ed.), *The Routledge handbook of new security studies* (pp. 50-58). London and New York: Routledge.

Den Boer, M. (1995). Moving between Bonafide and Bogus: The policing of inclusion and exclusion in Europe. In R. Miles, & D. Thränhardt (Eds.), *Migration and European integration: The dynamics of inclusion and exclusion* (pp. 92-111). London/Madison: Pinter Publishers/Fairleigh Dicksinson University Press.

Den Boer, M. (1998). Crime et immigration dans l'Union européenne. *Culture et Conflits, 'Sécurité et Immigration'*. Paris: l'Harmattan, n°31-32, 101-123.

Den Boer, M. (2003). 9/11 and the Europeanisation of anti-terrorism policy: A critical assessment. *Notre Europe*. Paris: Policy Papers no. 6.

Den Boer, M. (2008). Immigration and its effects on the security discourse in Europe: Time for demystification. *Amsterdam Law Forum*, *1*(1), 53-64.

Den Boer, M. & Buuren, J. van (forthcoming), *Door het oog van de staat*. Amsterdam: Boom.

Drent, M., & Zandee, D. (2010). *Breaking pillars. Towards a civil-military security approach for the European Union*. The Hague: Netherlands Institute of International Relations Clingendael (Clingendael Security Paper No. 13).

Easton, M., Boer, M. den, Janssens, J., Moelker, R., & T. Vander Beken, (forthcoming) (Eds.), *Blurring Military and Police Roles*. The Hague: Eleven International Publishing.

Gill, P. (2006). Not just doing the dots but crossing the borders and bridging the voids: Constructing security networks after 11 September 2001. *Policing & Society*, *16*(1), 27-49.

Gilleir, F., Easton, M., Ponsaers, P., & Cools, M., (2009). Checking aspects of a 'Nodal Orientation' for policing the Port of Antwerp. In M. Cools et al. (Eds.), *Governance of Security Research Paper Series: 2. Readings on Criminal Justice, Criminal Law & Policing* (pp. 359-376). Antwerp: Maklu.

Haggerty, K. (2009). 'Ten thousand times larger …': anticipating the expansion of surveillance. In Goold, B.J. & D. Neyland, (Eds.), *New Directions in Surveillance and Privacy* (pp. 159-177). Devon: Willan Publishing.

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

Held, D., & McGrew, A. (2007). *Globalisation theory: approaches and controversies*. Cambridge: Polity 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.

Huysmans, J. (2006). *The politics of insecurity. Fear, migration and asylum in the EU*. London: Routledge.

Ioannides, I. (2009). European Union security sector reform policy. What added value? *Eyes on Europe*, Autumn 2009, 37-41.

Johnston, L. (2002). *The rebirth of private policing*. London: Routledge.

Johnston, L., & Shearing, C. (2003). *Governing security*. London: Routledge.

Jones, T., & Newburn, T. (1998). *Private security and public policing*. Oxford: Clarendon Press.

Kaldor, M. (2008). From just war to just peace. In J. De Wilde & M. Den Boer (Eds.), *The viability of human security* (pp. 21-46). Amsterdam: Amsterdam University Press.

Kessler, O. (2010). Risk. In P. Burgess (Ed.), *The Routledge handbook of new security studies* (pp. 17-26). London and New York: Routledge.

Klerks, P. (2007). Methodological aspects of the Dutch national threat assessment. *Trends in Organized Crime*, *10*(4), 91-101.

Krahmann, E. (2005). Regulating private military companies: What role for the EU? *Contemporary Security Policy*, *26*(1), 1-23.

Lazarus, L., & Goold, B.J. (2007). Introduction: Security and human rights. In B.J. Goold & L. Lazarus (Eds.), *Security and human rights* (pp. 1-24). Oxford and Portland, Oregon: Hart Publishing.

Loader, I., & Walker, N. (2001). Policing as public good: Reconstituting the connections between policing and the state. *Theoretical Criminology*, *5*(1), 9-35.
Lutterbeck, D. (2005). Blurring the dividing line: The convergence of internal and external security in Western Europe. *European Security*, *14*(2), 231-253.
Medcalf, J. (2008). *Going global or going nowhere? NATO and the management of post-Cold War international crises*. Bern: Peter Lang.
NATO Allied Command Transformation (2008). *Multiple Futures Project. Project Initiation Document (PID)*. Version 1.5, April 2008.
Neyland, D., & Goold, B.J. (2009). Where next for surveillance studies? Exploring new directions in privacy and surveillance (Introduction). In B.J. Goold & D. Neyland (Eds.), *New directions in surveillance and privacy* (pp. xv-xxvii). Devon: Willan Publishing.
Owen, T. (2010). Human security. A contested contempt. In P. Burgess (Ed.), *The Routledge handbook of new security studies* (pp. 39-49). London and New York: Routledge.
Ramraj, V.V. (2007). Between idealism and pragmatism: Legal and political constraints on state power in times of crisis. In B.J. Goold & L. Lazarus (Eds.), *Security and human rights* (pp. 185-202). Oxford and Portland, Oregon: Hart Publishing.
Ryngaert, C. (2008). *Private military contractors: Regulatory options*, Policy Brief No. 5, Leuven, Leuven Centre for Global Governance Studies, www.globalgovernancestudies.eu.
Sackers, H.J.B. (2010). *Herder, hoeder en handhaver. De burgemeester en het bestuurlijk sanctierecht*. Inaugural speech Radboud Universiteit Nijmegen, Nijmegen, 15 January 2010.
Schreier, F., & Caparini, M. (2005). *Privatising security: Law, practice and governance of private military and security companies*, Occasional paper at DCAF, Geneva, www.dcaf.ch/_docs/occasional_6.pdf (www.dcaf.ch/publications).
Shearing, C., & Stenning, P.C. (Eds.) (1987). *Private policing*. London: Sage.
Shearing, C., & Wood, J. (2007), *Imagining security.* Collumpton, Willan Publishing.
Van Buuren, J. (2009). *Security as a commodity. Ethical dilemmas of private security*. Brussels: INEX.
Vander Beken, T. & Verfaillie, K. (2010). Assessing European futures in an age of reflexive security. *Policing and Society*, *20*(2), 187-203.
Van der Wal, Z., & Huberts, L. (2008). Value solidity in government and business. Results of an empirical study on public and private sector organizational values, *The American Review of Public Administration*, *38*(3), 264-285.
Van Steden, R., & Sarre, R. (2007). The growth of privatized policing: Some cross-national data and comparisons. *International Journal of Comparative and Applied Criminal Justice*, *31*(1), 51-71.

White, N. D., & MacLeod, S. (2008). EU operations and private military contractors: Issues of corporate and institutional responsibility. *The European Journal of International Law*, *19*(5), 965-988.

Wood, J. & Shearing, C. (2007). *Imagining Security*. Devon: Willan Publishing.

Zedner, L. (2006). The concept of security: An agenda for comparative analysis. *Legal Studies*, *23*(1), 153-176.

Zedner, L. (2007). Seeking security by 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.