Private security regimes: Conceptualizing the forces that shape the private delivery of security

Benoit Dupont

Theoretical Criminology 2014 18: 263 originally published online 21 March 2014
DOI: 10.1177/1362480614527303

Article

Theoretical Criminology
2014, Vol. 18(3) 263–281
© The Author(s) 2014
Reprints and permissions:
sagepub.co.uk/journalsPermissions.nav
DOI: 10.1177/1362480614527303
tcr.sagepub.com
SAGE

Private security regimes: Conceptualizing the forces that shape the private delivery of security

Benoit Dupont
Université de Montréal, Canada

Abstract

There is as much diversity within the private security industry as there are differences between public and private security providers. Whereas comparisons of the two modes of delivery have kept criminologists and economists fairly busy over the years, internal variations have not attracted the same level of interest. In the current environment, binary classifications such as the public/private security dichotomy might be too generic to capture the broad spectrum of unique security arrangements being adopted by various organizations. The aim of this article is therefore to offer an alternative conceptual framework that can account for the broad range of mechanisms responsible for the diversity of private security arrangements observed in late modern societies. The term 'security regime' defines the convergence of internal forces and environmental constraints that determine the conditions under which security is produced and exchanged by an organization. The four key dimensions (focus, risks, utility and constraints) that characterize a specific security regime were identified from interviews conducted with more than 50 security managers. The security regime approach should expand our knowledge of the various causes that facilitate, empower or hinder public–private relationships.

Keywords

Constraints, governance, regulation, risks, security, utility

Corresponding author:
Benoit Dupont, International Centre for Comparative Criminology, Université de Montréal, CP 6128 succ. centre-ville, Montreal, QC H3C 3J7, Canada.
Email: benoit.dupont@umontreal.ca

There is as much diversity within what is commonly referred to as the private security industry as there are differences separating public and private security providers. Whereas quantitative and qualitative comparisons of the two modes of delivery have kept criminologists (Brodeur, 2010; De Waard, 1999; Johnston, 1999; Loader and Walker, 2007; Shearing and Stenning, 1987; Van Steden and Sarre, 2007), economists (Bartel, 1975; Becker, 1974; Clotfelter, 1978; Cook and MacDonald, 2011; Cunningham et al., 1990; Friedman et al., 1987) and even several political scientists (Abrahamsen and Williams, 2011; White, 2011) fairly busy over the years, internal variations have not attracted the same level of interest despite their potential for shedding light on the conditions of security production in late modern societies. Indeed, the work of high-end private security contractors training and escorting NGOs' employees in conflict zones (Avant and Haufler, 2012) or negotiating the release of abducted company executives in fragile states (O'Reilly, 2011) bears little resemblance with the daily tasks of a shopping mall 'ambassador' or a computer security consultant. Yet, all these functions are usually lumped together under the private security label.

Hence, in the current environment, binary classifications such as the public/private security dichotomy might be too generic to capture the broad spectrum of unique security arrangements being adopted by various organizations and institutions. In Montreal for example—as in many other places around the world— while the local police sells some of its services to private interests, private security guards have taken over low-level public security functions such as by-law enforcement and park patrols in certain boroughs. Furthermore, the assimilation of private security to a typical market exchange where a solvent buyer meets an enterprising seller does not reflect the more complex nature of certain exchange structures such as two-sided markets, where there is not a single end-user (or customer) but two (Rochet and Tirole, 2006). Private security is not a two-sided market per se, but manages the risks inherent to these particular economic configurations. Shopping malls are an archetypal example, where guards provide their services to retailers and consumers on behalf of malls' owners and must sometimes reconcile the conflicting security needs of both sides (Van Steden, 2007; Wakefield, 2003). It is indeed vital for malls' management to balance the satisfaction of retailers and patrons in order to maintain high levels of rental occupancy and attendance, because the demand from one side diminishes if the other is not there (customers will not come if security is too aggressive or visible, and retailers will choose a competing mall if their employees and customers feel unsafe). A similar situation exists in the payment card industry, where fraud management must deal with the conflicting rationalities of card holders (protection against losses) and merchants (speed and ease of transactions), which nevertheless both represent a source of profit for card issuers (Evans and Schmalensee, 2005: ch. 6). This blurring of the lines highlights the need for a more detailed understanding of the multiple dimensions that shape the private delivery of security, not only to understand what it is that particular providers actually do, but also why and how they do it.

The literature has so far examined some of those dimensions separately, outlining for example typologies of private security tasks and functions (Brodeur, 2010; Cunningham et al., 1990; Cusson and Diotte, 2007; NACCJG, 1976; Rigakos, 2005), or mapping the various regulatory forces that constrain private providers (Button, 2007; Davis et al., 2003; O'Connor et al., 2008; Prenzler and Sarre, 2008; South, 1988; Stenning, 2000;

White, 2010). However, the various dimensions have not been integrated into a single analytical model, despite the complex web of interdependencies that bind them together. Another approach has been to conduct in-depth analysis of security provision in specific settings such as amusement parks (Shearing and Stenning, 1987; Van Steden, 2007), shopping malls (Van Steden, 2007; Wakefield, 2003), large retail stores (Ocqueteau and Pottier, 1995), the night-time economy (Hobbs et al., 2003), sports events (Manning, 2006; Van Steden, 2007), public housing (Rigakos, 2002) and so on. These case studies, although very detailed, are necessarily limited in their scope and can only explain how some subsets of the private security sector operate.

The aim of this article is therefore to merge the two approaches in order to assemble a conceptual framework that will embed the broad range of mechanisms responsible for the diversity of private security arrangements observed in late modern societies. The analytical strategy adopted here is very sympathetic of Valverde's (2010) call for a more open-ended and content-neutral framework, which would be more useful than general theories of security to explore the inherently plural, unstable and contradictory nature of security projects. In the remainder of this article, I use the term 'security regime' to describe the convergence of internal and environmental forces and constraints that determine the conditions under which security is produced and exchanged by an organization. A security regime will not only frame an organization's security mandate and the acceptable means that can be mobilized as a result. It will also define its ability to collaborate, compete or struggle with other organizations. In that sense, it is not limited to a static description of structural features, but also embraces the dynamic nature of plural security delivery.

The private security regime framework was built inductively from interviews conducted with security managers from private and parapublic organizations. The data collection methodology and features of the sample are discussed in the first section of this article. In the following section, the four key dimensions of security regimes (focus, risks, utility and constraints) are outlined and illustrated through several examples. I conclude by showing how private security regimes influence security outcomes and in particular might explain why partnerships are so central to private security work. In a world where public and private security organizations interact increasingly through a complex web of linkages (Ayling et al., 2008; Bayley and Shearing, 2001; Dupont, 2004; Johnston and Shearing, 2003; Loader and Walker, 2007; Mazerolle and Ransley, 2005; Wood and Shearing, 2007), the security regime approach should expand our knowledge of the various causes that facilitate, empower or hinder these relationships, beyond the descriptive benefits associated with a more nuanced understanding of private security delivery.

The Montreal case study

The security regime framework derives from a research project conducted over a 17-month period (January 2004 to May 2005) in Montreal, a Canadian city of 1.8 million people that in many aspects resembles other urban centres in the western world: its manufacturing base is eroding and being replaced by a knowledge economy. Large cities such as Montreal are also characterized by complex spatial-institutional patterns that include (but are not restricted to) mass private properties, transport hubs, corporate headquarters, government buildings or privately organized street festivals. As a result, these sites of production, consumption and leisure require security arrangements that transcend the classical public police/private security dichotomy. In order to understand how these arrangements emerge and what main variables influence their organization and operations, 52 security managers from a diverse range of public, parapublic and private organizations answered open-ended questions related to their security mandate, the various types of resources that could be mobilized to meet these objectives, the constraints encountered in the process, their own personal experience in the security field, the sources of their knowledge and the benefits and challenges deriving from their interactions with other security actors. The term 'security manager' as it is used here includes both employees of private security companies and of large organizations (banks, retailers, museums, hospitals, etc.) who purchase security services and goods in order to manage their employer's risks. Additional interviews were also conducted with five police executives to explore the nature and extent of linkages maintained with other security organizations.

Although the interviews upon which the security regime typology is based are almost a decade old, a period that has seen the US and many European economies devastated by a long and painful recession, I believe that the data presented here are still relevant: first, they are not used to illustrate a particular cyclical trend such as decommodification or insourcing (Lippert et al., 2013), but to discover a limited set of stable variables that influence the complex security provision arrangements found in contemporary societies. The relative importance of these variables will inevitably change over time, but their overall structure should remain the same. Additionally, while police organizations in the UK, the USA and many other countries have experienced severe budget cuts since 2008, the private security sector has managed to ride out the financial storm with surprising ease. If the global market for private security services experienced a slight decline in 2009 (–4 per cent), it quickly recovered the following year to a 4.7 per cent growth rate (Datamonitor, 2011: 9), and is forecast to sustain an average annual growth rate of 4.9 per cent between 2012 and 2017 (MarketLine, 2013: 13). In the USA, the main industry association estimated that private security spending grew by 5.5 per cent in 2013 (ASIS International, 2013), while in the UK, after having experienced a 3 per cent decline in 2009, the manned security industry was forecast to see annual growth fluctuating between 2 per cent and 4 per cent from 2011 to 2015 (Sims, 2010). Canada's economy experienced a shorter and milder recession that has left the private and corporate security sectors relatively unscathed, and nothing suggests in my follow-up interactions with a large number of respondents whom I meet occasionally at industry conferences that what they described a decade ago does not apply anymore.

The sample

As can be expected in such a traditional occupational field, respondents are predominantly males (77 per cent). The respondents' professional experience in the security sector averaged 20.2 years, with only 37 per cent having completed a university degree. The proportion of security managers with a previous police experience amounts to 31.9 per

Table 1. Respondents' organizational affiliation.

	N	%
Public police	5	9.5
Parapublic sector	21	40.5
Professional and trade associations	1	2
Private security		
In-house	16[a]	31
Contract/generalist	3	5.5
Contract/investigations and expertise	4	7.5
Contract/equipment	2	4
Total	52	100

Note: Percentages are rounded.

[a] The organizations from which the sample of in-house security managers were drawn included two conference and concert venues, three office and retail complexes, a music festival and concert promoter, two banks, two pharmaceutical companies, a national broadcaster, an aerospace manufacturer, a mining conglomerate and two large retailers.

cent. Such a high rate of personnel movement from public to private security proves very similar to what Shearing and Stenning (1983: 503) observed 30 years ago in Ontario, and probably reflects in part the resilience of what White (2011: 89) describes as 'conscious efforts to create a general impression of "stateness"'.

The organizations from which data were collected can be grouped in seven main categories, which are defined institutionally and functionally. The first dimension is institutional, and distinguishes whether security is considered as a public good (delivered either by the police or other state entities) or a private effort. It also lets us incorporate professional and trade associations, which are neither public agencies nor private corporations, but nevertheless play an important role in the security ecology. The parapublic sector is certainly the hardest category to delimit. It refers to government agencies that have law enforcement powers, which Jones and Newburn (1998:136) identify as 'other public policing bodies' and that include for example public transport security units, social benefit fraud investigators as well as various safety and security regulatory bodies. This category also comprises institutions that are resourced by public monies but do not necessarily possess any special enforcement powers, such as universities, museums or hospitals. All these organizations have a physical footprint that requires some form of security. The second dimension is by nature functional and essentially applies to private modes of delivery. It differentiates in-house security, where companies meet their own security needs, from outsourced security, where specialized businesses are called in to provide security on a contractual basis. The typology further differentiates three types of contract security, because of the high level of variance between the practices associated with each of them. Table 1 summarizes the distribution of respondents within each category.

The 47 organizations that employ the respondents account for more than 18,000 security-related jobs within the city's geographical boundaries. This sample of security providers cannot make any claim to statistical representativeness, but the employee data suggest it nevertheless includes a significant segment of the industry in the reference area.

Because of their responsibilities, the respondents had extremely busy workdays, and unexpected circumstances often led to the cancellation and rescheduling of appointments, which accounted for the extended data-gathering period. Interviews lasted an hour and 15 minutes on average (range: 40 minutes–two hours), and all were recorded and transcribed for coding, with the exception of two respondents who refused to be taped and for whom extensive notes were taken. The qualitative analysis was carried out with the QDA Miner software package.

The four key dimensions of private security regimes

Instead of assuming that security organizations belonging to the typology outlined in the previous section pursue distinct objectives and strategies primarily defined by their structural features, I adopt a modular approach that reflects the highly instrumental nature of private security work (Shearing and Stenning, 1983: 500). Although the profit motive can explain some of the underlying principles that shape security work (Rigakos, 2002; Spitzer and Scull, 1977; Zedner, 2009), it needs to be complemented by additional dimensions that can also apply to organizations that are not fully private. Some public and parapublic organizations offering access to government services such as health or education might for example resort to private security guards in order to protect their employees, their users or their assets, and will expect their contractors to conform to their particular public mandates when performing their tasks.

An alternative explanation to these disparities could find its roots in the manifestation of personal preferences, where some security managers lean towards a preventative stance while others favour a more repressive attitude modelled on police work that can culminate with the 'parapolicing' practices observed by Rigakos (2002) in Toronto, and by Berg (2010) and Marks and Wood (2007) in South Africa. Although the impact of such personal tastes—shaped by previous experiences in public policing for example—should not be discounted, variations in security delivery are justified in much more pragmatic terms by security executives. They reflect local organizational needs and constraints—rather than universal norms and standards, dictating what levels of security are required (and acceptable), by what means those objectives are to be met and what criteria are used to assess outcomes.

Four main sets of variables emerged as key components of local security regimes under which executives operate. These four sets of variables are: the people, places and flows that need to be protected (the focus of security); the risks (real or imagined) against which protection is required; the utility assigned to security functions; and the particular constraints which are experienced in the course of addressing those risks. The numerous permutations made possible by these four groups of forces and constraints (and their subcomponents) respond to narrow local and organizational needs, resulting in a diversity of highly contextual security regimes.

The focus of security: People, places and flows

First of all, the security arrangements of an organization are strongly influenced by its determination of whom and what warrants its protection. The three main foci of an organization's security activities mentioned by respondents were people, places and flows. Of course, they are closely connected to each other, so much so that it often creates tensions and even contradictions that are not easily resolved.

The focus on 'people' covers a broad range of individuals whose ties with the security providing organization can be more or less formal, but who nevertheless expect to conduct their dealings in a safe environment. Employees, public service users, as well as various types of customers are all indirect beneficiaries of privately provided security arrangements that must often reconcile contradictory needs through ad hoc negotiations. Health workers are a good example: they are particularly exposed to workplace violence and to assaults from patients and their families (Graham and Shirm, 1995; Shields and Wilkins, 2006). As a result, hospital security frequently involves the use of coercive force, but the duty of care owed to patients creates challenging dilemmas for those in charge. In contrast, security provision in retail and leisure environments is characterized by its customer service approach which must balance a reassuring presence with the need to remain as unobtrusive as possible in order not to spoil the patrons' experience (Van Steden, 2007; Wakefield, 2003: 119). This customer focus is however very selectively directed towards consumers who are perceived as 'legitimate' and 'respectable', while those whose behaviour or consumption patterns do not conform with accepted norms are routinely excluded from privately operated communal spaces (Huey et al., 2005).

By the same way that people-focused security measures involve considerable variations in terms of coerciveness and intrusiveness, the relationship between places and security can also induce substantial differences in the delivery of security services. One common method to analyse space is to build a continuum where one extremity consists of private places that can only be accessed by personal invitation (dwellings), and the other end represents public spaces whose access is in theory unconditional (streets and public parks). In the middle, one can find communal spaces that are usually (but not always) privately owned but are nonetheless open to the public on the proviso that certain rules such as the purchase of a valid ticket or compliance with tacit norms of conduct are accepted (Kempa and Singh, 2008: 335). Shearing and Stenning (1981) have perhaps provided the most influential account of the role 'places' play in the security realm when they argued that the development of a particular form of privately owned public space known as 'mass private property' was responsible for the rise of the contract security sector towards the last quarter of the 20th century. In order to determine where on the continuum a particular place should be positioned, various criteria can be used such as the categories of people who can routinely access it and its ownership structure (Wakefield, 2003: 24), the kinds of systems that are used to control its access (Jones and Newburn, 1998: 51) or the 'institutional DNA' of the organization defining the order enforced in this particular space (Kempa et al., 2004: 570). This 'accessibility test' is important, because the level of openness of a place is tightly coupled to the actual power exercised by those who secure it: while more enclosed and restricted spaces make it easier for guards and their managers to undertake their tasks without being challenged, the scope of their operational freedom narrows considerably in communal and public spaces, where they must negotiate with the police (Brodeur, 2010: 280), their unions and the sometimes recalcitrant public (Bellot and Cousineau, 1996; Ocqueteau and Pottier, 1995: 177) what they can and cannot do. Finally, the protection of places provides the same fertile ground for dilemmas and tensions between conflicting interests that was observed for the protection of people. Some places require at the same time a high level of security and accessibility, despite the obvious contradiction between the two. Museums are a particularly good example of this conundrum.

In contrast with people and places, flows are characterized by their intangibility, which makes them much harder to monitor and ultimately secure. The flows of goods, services and data that irrigate globalized markets are vital assets for companies that operate in highly competitive environments. A growing proportion of security executives are not only responsible for their company's employee and building security, but also have to protect the blueprints, formulas, algorithms, experiments, models and valuable ideas produced by those employees. One security manager from the pharmaceutical industry explained for example how the well-documented practice of leaving tickets or 'snowflakes' (Shearing and Stenning, 1983: 499) on the desks of employees who had failed to secure confidential documents at the end of their work day was complemented by random inspections of electronic communications going through the company's computer firewall, in order to verify that classified information or 'close to completion' research was not improperly disseminated.

The risks portfolio

Although risks are intricately tied to the particular people, places or flows that are exposed to them, they need to be analysed separately in order to understand how specific risks shape security outcomes. It is almost irrelevant whether these risks are real or imagined, as long as their probability of materializing and their hypothetical fallout are viewed by decision-makers as exceeding the capacity of the organization to absorb them without particular security measures. Button (2008: 126–127) shows how risk profiles vary from one context to another, and how various organizational contexts have a very different tolerance for risk, based on the level of security required and the intensity of commercial pressures at work. His analysis highlights the complexity (some would argue the futility) of risk assessment and management procedures within modern security organizations. However, most of the risks considered in Button's model are of a criminal or terrorist origin. If the surveyed security executives were indeed actively engaged in the management of these high profile risks, their risk portfolio also included a broad range of perils that hardly lend themselves to straightforward cost–benefit analysis.

Criminal risks. Depending on their core activities, public and private organizations can represent an attractive target for offenders, from the petty theft of insiders (Ditton, 1977) to the more heavy-handed tactics of organized crime (Van Duyne, 1993). Overall, 23 per cent of respondents mentioned the risk of theft among their top priorities. However, contrary to a widely held belief (Brodeur, 2010: 279), private security must not only deal with threats to property but also with frequent occurrences of violent incidents ranging from intimidation and harassment to assault and even homicides. These risks involve an organization's employees, users and customers in different combinations that are specific to each setting (Boyd, 1995; Castillo and Jenkins, 1994; Kraus, 1987). One in four respondents (25 per cent) mentioned risks associated with physical violence in their interviews. Unlike criminal risks of an acquisitive nature, violence risks are mostly addressed through the involvement of the police, even if managers admitted that the decision rested mostly in the hands of the victim. Health sector respondents had implemented the most formalized intervention strategies:

> At [our] hospital for example, interventions have increased by 20 per cent a year over the past four years. That means we carry out an average of 1000 physical interventions a year. Patients can be overdosing on drugs or experiencing alcohol-related problems, domestic violence, or suffer from psychiatric episodes. Our security guards belong to an intervention group, which usually consists of no less than four people: two agents and two hospital employees. An ideal situation is to have six people available for an intervention.
>
> (#29)

Terrorist risks. Even if the chances of being exposed to a terrorist event remain very slim for an organization operating outside a conflict zone (including airlines), the 9/11 attacks and the subsequent bombings carried out in the Madrid and London public transport systems in 2004 and 2005 have compelled many respondents to update their security arrangements hastily. Some organizations discovered that they had delayed security investments for a number of years and that their infrastructures were inappropriate to address any serious threat to their operations. The security manager of a public transportation company described for example how 9/11 acted as a catalyst for his employer, which had left the position vacant for two and a half years. This example, which is far from unique, typifies how low-probability/high-severity risks have a tendency to become ‘orphan risks’ (i.e. neglected until a crisis strikes) in operational environments where security investments are always assessed against more directly productive assets.

Competitive risks. In the current highly competitive global business environment, knowledge assets such as patents, know-how, processes, designs and ongoing research projects represent attractive targets for aggressive rivals that wish to acquire and market the latest technologies with the least efforts. For those who must protect these assets, things are not so simple and constant compromises must be made between security and openness, one of the key features of the information society (Nasheri, 2005) and one of the main productivity and innovation drivers. From a security perspective, competitive risks are difficult to manage as insiders who can inflict the most damage from negligence or malfeasance are also those who can most safely resist compliance due to their hierarchical position.

Occupational health and safety risks. Because it emphasizes comparisons with the public police’s functions and means, the private security literature tends to underestimate a whole class of risks that has more to do with health governance and workplace safety than with policing. In-house and contract security personnel are indeed routinely tasked with a broad range of occupational health and safety (OHS) duties that include fire prevention, the management of hazardous materials and waste, compliance to building regulations and various local and national OHS policies, accident prevention, first aid interventions and liaison with ambulance services. Indeed, 42 per cent of respondents were involved with the management of this diffuse category of risks and it was so central to the core functions of some of them that their position was primarily defined by this mandate, security being relegated to a subsidiary role. As a result of this routine involvement in OHS risk management and fire prevention activities, private security managers are embedded in labour and fire regulatory networks that include compliance and enforcement agencies, insurance companies, industry associations and technology and training providers (Bartrip and Fenn, 1983; O'Malley and Hutchinson, 2007).

Catastrophic risks. A fifth category of risks confronted by a significant proportion of security managers involves events whose disruptive potential is large enough to threaten the organization's survival. Such events include natural disasters, industrial accidents, pandemics or human stampedes. One-third of respondents (32 per cent) stated that their responsibilities incorporated this category of risks, for which they admitted their resources were probably inadequate. Two commonly mentioned strategies used to overcome this discrepancy between needs and means were contingency plans grounded in realistic expectations and trusted relationships with key partners that would facilitate the pooling of scarce resources in crisis situations.

Reputational risks. Not all risks faced by an organization are as tangible as criminal offending, terrorist attacks or natural disasters. The reputation of a company represents a valuable asset that can quickly become a liability when the erosion of customers' and suppliers' trust provokes a loss of competitiveness. Shareholders are also very receptive to such signals and several security managers explained how their performance was indirectly tied to their company's public valuation. The ambiguity that characterizes this risk category explains why contract security firms providing investigative and consulting services of all sorts are routinely called in before the police—when the police is involved at all—in order to minimize external scrutiny and to maximize procedural control (Gill and Hart, 1999: 252; Williams, 2005). Overall, 15 per cent of respondents mentioned this particular category of risks.

Faced with such an abundance and diversity of risks, some of them being incommensurable to the available response capacities, security managers resort to ad hoc—or even haphazard—arbitrages that are contextual and very unstable in order to allocate and to prioritize limited resources. As seen, these decisions create orphan risks or lead to the transfer of a risk from one category to another, therefore resulting in security arrangements whose configuration is constantly being redefined. What does not appear in this short typology but was nevertheless frequently expressed by frustrated respondents was the fact that risks are interpreted differently throughout the organization. What is perceived as a threat by security managers can represent a business opportunity for marketing executives (Favarel-Garrigues et al., 2008) or nurture the creativity and innovativeness of R&D divisions. For an organization, defining and managing risks is rarely a consensual affair.

The utility of security

It would be reductive to restrict the utility of security to risk management functions, no matter how diverse they prove to be. Obviously, in-house or contract security services contribute to the bottom line by minimizing losses caused by theft, vandalism, negligence or accidents. But beyond protective tasks, security workers also undertake a range of assignments whose utility extends from the provision of customer service to the management of human resources and can even involve various forms of regulatory misconduct.

The customer service utility of security is often underestimated by private security scholars who tend to emphasize coercive and surveillance activities. The empirical work of Huey et al. (2005), Van Steden (2007) and Wakefield (2003) provide notable exceptions to this approach. Their ethnographic observations of shopping malls and amusement parks uncover practices that tend to tone down the most visible manifestations of security work in order to dilute any reminder of disorder that could make customers uncomfortable. This perspective is slightly different from the ‘Disney order’ depicted in Shearing and Stenning (1987), where every park employee is engaged in order maintenance functions. Here, it is security employees who must indirectly fit within the customer service ethos of their employer. In this research, one art museum security manager fully embraced this rationale by training security guards to provide basic information to visitors about the paintings and installations they came to see:

> We worked quite hard over the previous years to be more convivial, so that visitors would feel welcome by security and other people working here … We train our security guards to interact with the public. This is not an art history course, but it provides them with basic knowledge, and sometimes we even arrange for them to meet artists … They [guards] are not expected to describe the political or social meaning of a piece, but they should be able to explain what it is and to what exposition it belongs to.
>
> (#50)

This example provides a good illustration of the extent to which security is often redefined at the local level according to its perceived organizational utility. An extreme manifestation of this service utility can be found in the personal protection security business, where the provision of expensive bodyguards implicitly incorporates a broad range of services that seem more familiar to the hospitality industry than to the security sector. One respondent was particularly candid in his assessment of this type of arrangement:

> A company executive who pays you 100,000 CAD a year wants to get value for money. He wants you to make sure he can always find a table at a restaurant, because you have become a personal protection adviser. He wants his car to be waiting for him when he needs it, and he wants it to be comfortably warm. You basically become a lackey.
>
> (#27)

Allusions were also made to the not uncommon occurrence of having to arrange at very short notice the sexual services of exclusive escorts, where the main obvious security component of the task was protection against the enquiries of suspicious spouses.

The usefulness of security was also extended by several respondents to the human resources area. Security personnel involvement in labour relations has always been a contentious issue (Spitzer and Scull, 1977; Weiss, 1987). Today, private security managers continue to play an important role in human resources, not as enforcers of their employer's order (even if 'strike management' services can still be obtained from specialized private security outfits) but as intelligence brokers and negotiators. A growing number of companies require that their new hires undergo some form of background check (also called pre-employment screening in Canada) performed by in-house investigators or through a third-party provider. It is also common for government and parapublic agencies to hire private investigators for cases that involve sensitive employees such as union representatives or high ranking officials. One respondent (#36) who provided such services explained that his clients had the internal resources to undertake these investigations but preferred to outsource to the private sector in order to avoid leaks. In one of the most extreme cases of this trend, the Montreal daily *La Presse* revealed in early 2011 that the city comptroller had hired a private security company to investigate the chief of police (De Pierrebourg and Noël, 2011). When insider thefts are involved, private security managers must often communicate the evidence to the human resources department, which will decide whether to sue the employee, to dismiss him or her or to impose alternative remedies. One security manager (#46) operated in a retail environment where the union was so powerful and uncompromising that he had been selected because of his extensive knowledge of the local industrial relations regulatory framework.

The final utility alluded to in the interviews involves a protective component, not from criminal or natural risks but from the norms and institutions that regulate business conduct. Although none of the respondents admitted openly to unlawful practices undertaken on behalf of a client or to protect their company, a few evoked the tension between the loyalty towards private interests and the common good, which can often be in contradiction. The contract security companies specializing in investigations seem to be the most exposed (Gill and Hart, 1999: 255), mainly because of their small size, the intense competition that prevails in this market, the opaqueness of their mandates and the plausible deniability they offer to customers if they get caught. In some extreme cases, large companies have been caught using their own security services or contractors to cover up systematic compliance evasion practices or to launch aggressive intelligence gathering and smear campaigns against competitors, NGOs and government officials (Crawford, 2009; Darlin, 2006; Permanent Subcommittee on Investigations, 2008: 98; *The Economist*, 2009). Even if the convenient 'rotten apple' argument is systematically invoked by those exposed corporations, it is not unreasonable to assume that these questionable practices are quite common (South, 1988: 102; Zedner, 2009: 98). Therefore and ironically, one organization's security resources can easily be mobilized to generate insecurity for its economic, social or political rivals.

The proliferation of constraints

The previous three dimensions provide a useful lens to understand how local security regimes emerge in response to specific risks and needs. But the significant role played by internal and external constraints should also be examined thoroughly, as it reveals how contextual factors constantly hinder security policies and lead to compromises that limit their reach. This is the fourth dimension of security regimes. The interviews revealed that, far from assuming a hegemonic position within their organizational structures, security units and their managers often needed to deploy large amounts of energy and social capital to convince other members of the organization to adopt security-compliant practices, especially in workplaces where the dominant culture emphasizes risk-taking, effectiveness, innovativeness or customer satisfaction.

Constraints can be of a geographical, functional, financial, technological, legal or cultural nature. Geographical constraints are particularly pronounced for organizations that must secure a large number of dispersed sites across the world. A respondent (#43) was for example responsible for the design of risk management policies that needed to be implemented across 500 plants on the five continents. The geographical scope of such mandates significantly complicates the co-ordination of security activities in a sector of the economy where providers and regulatory frameworks are mostly local.

The functional constraints derive from the fact that, even if security is frequently integrated with other organizational functions such as sales or human resource management (Shearing and Stenning, 1983: 499), the relationship between security and core activities is not always straightforward or without complications, as I have already suggested in the section on risks. Even security can be broken up at the operational level into discrete areas of expertise that cover specific assets and activities, especially in large institutions that deploy complex physical and informational systems. Banks offer a good illustration of these functional constraints: their diversified risk portfolio generates an ad hoc segmentation of tasks. Physical security is for example focused on deploying alarm and CCTV systems characterized by a strong engineering component (#34), while the anti-fraud function mobilizes traditional investigative skills that are supported by sophisticated computerized tools such as data mining and artificial intelligence software (#28). Anti-money laundering efforts also mobilize some specialized investigative expertise, but the latter is complemented by auditing, compliance and account management skills (Favarel-Garrigues et al., 2008; Gill and Taylor, 2004). The fragmentation of security functions within large organizations generates ownership challenges that often result in sub-optimal co-ordination.

Financial constraints reflect the low organizational status held by in-house security units and the thin profit margins enjoyed by contract security firms. Respondent #12, a university security manager, was appalled to discover after his appointment that salaries consumed 99.2 per cent of his budget. Many other respondents expressed their frustration about the administrative hurdles they had to overcome in order to see basic budgetary requests approved, needing to show how security expenses could provide a satisfactory rate of ROI (return on investment). In a hospital setting (#29), CCTV systems were delayed for several years because expensive medical equipment such as scanners and MRIs took precedence.

In *The Policing Web*, Jean-Paul Brodeur (2010: 255 and 276) laments the lack of interest displayed by private security researchers in the technology and equipment segment of the industry, despite its large market share and fast growth. For security managers, the limitless number of technological solutions available to them introduces an additional constraint. These systems are always expensive, even if the marketing arguments used to promote them emphasize the savings they can generate over more traditional manned arrangements. In the frugal financial context highlighted above, there is a fundamental tension between the scarce resources available to purchase security technologies and the constant flow of new products inundating the market. Procurement decisions are therefore preceded by a research phase that seeks to avoid costly mistakes. Security managers try to establish whether the technology they covet can be integrated with existing or legacy systems (#42), or to what extent it can deliver on the hyperbolic promises made by sales people. Several respondents (#1, #4, #11) mentioned the uncertainty and stress associated with such purchases and how they leveraged their networks in order to decode the technical jargon used by suppliers, or to verify their reputation. In certain sectors of activity such as the banking, defence or air travel industries, security technologies must comply with technical standards defined by various regulatory authorities and insurers, leaving little flexibility to security managers operating in those areas. Despite the claims often made by the champions—and detractors—of security and surveillance technologies regarding their social control efficiency, their selection and adoption by security professionals are often plagued by delays, defaults and disappointments.

Legal constraints define to a great degree what security tasks consist of, both in terms of what can and cannot be done. Legal constraints can apply directly to the organization, or can originate externally from a provider or a customer's particular regulatory environment. As Philip Stenning (2000) has already extensively reviewed the various legal constraints that hold the private security industry accountable (state regulation, industry self-regulation, criminal liability, civil liability, labour law and contractual liability), there is no need to duplicate his work here.

The final constraint encountered during the interviews is of a cultural nature (Nalla and Newman, 1990). If most organizations in the defence or banking sectors have developed through the years a certain degree of compatibility with extensive security requirements, other institutions are apprehensive or averse to the ostentatious display of security technologies and procedures. Organizations that emphasize core values such as ease of access, freedom of expression and creativity can prove challenging for security executives who must implement satisfactory levels of risk management while avoiding any perception of excessive control. Respondents working for media companies, social services, museum and educational institutions routinely had to defer to these cultural constraints, as this quote illustrates:

> Security must understand its role, which is a support role, in order to provide a secure environment to allow people to do what they have to do, professors to teach, students to study, visitors to visit, and to ensure that they do not feel threatened or intimidated. So our role is important, but it must be a self-effacing role. We must be there when we are needed, but we must not be an obstacle.
>
> (#12)

The six types of constraints listed above are characterized by a high level of interdependency. For example, geographical constraints are correlated with financial and regulatory constraints, and legal constraints related to privacy can significantly enhance technological constraints. Although some commonalities are to be expected among in-house security units and contract security companies that operate in similar environments, their work is mostly determined by a unique mix of constraints, utilities, risks and foci that are defined here as security regimes.

Conclusion

Through interviews with a diversified sample of security managers operating in a dense urban environment, this article highlights how security as an activity varies greatly from one organization to another. The observed variations provide a wealth of information, whose value has been underestimated, on the forces that shape security outcomes in late modern societies. The private security regime framework proposed here articulates how four main dimensions (focus, risks, utility and constraints) seem to determine to a large degree what level of security is deemed acceptable by a particular organization, and how specific security measures are designed, implemented and sometimes even resisted or evaded (Ocqueteau and Dupont, 2013).

The nature of an organization's security regime can help us understand why security managers with police backgrounds dominate certain organizations or alternatively, why candidates who can tap into their old boys' network are avoided in favour of executives who lay claim to more formal security knowledge. The intensity with which security technologies are used, the level of integration with other intra-organizational activities, the position within the institutional hierarchy (formal and informal) and even the propensity to use force derive to a large extent from the security regime under which a particular unit or business operates. It can also explain (at least in part) why some organizations outsource most—or all—of their security activities, while others retain a strong in-house capacity, for reasons beyond mere financial rationality.

From an inter-organizational perspective, security regimes influence autonomy or dependency. We could for example formulate the hypothesis that the types of partners selected by a security organization, the size and structure of its network or the strength of its external ties are to a certain degree correlated with particular features of its security regime. The sheer complexity that characterizes the numerous combinations and permutations allowed by the four dimensions highlighted above, coupled with the limited resources available to in-house security managers and the uncertainty attached to their mandate might also explain why the networked form of organization is so attractive to them (Dupont, 2006). In a very constrained environment, security networks allow managers to tap into a vast pool of knowledge, experiences and reliable contacts, in order to respond to the unique challenges that security regimes pose to them. As a consequence, those who seek to design, optimize or regulate security networks should pay particular attention to the security regimes associated with their most powerful nodes. It is probable that the most salient features of such regimes determine to a large extent the properties of security networks and the linkage (or conflict) strategies of their members.

But the security regime typology should not exclusively be understood as a mere extension of the network/nodal security approach (Johnston and Shearing, 2003; Shearing and Wood, 2003). The proponents of anchored pluralism (Loader and Walker, 2006), who are more sceptical of the nodal approach and favour the state as the meta-regulator of collective security provision, could also leverage the security regime framework to define better under what conditions (positive and negative) plural social and security identities can be embedded into a state defined ordering field, to borrow from their terminology. In other words, the security regime typology presented in this article is agnostic. Security regimes are not elegant theoretical constructs based on general principles that could neatly encapsulate the predictable features of private security provision. Instead, they provide us with a conceptual toolbox compatible with the complexity of current private security arrangements, whose rationalities are at best ambiguous and inconsistent, when they are not replete with contradictions.

Funding

This work was supported by the Social Sciences and Humanities Research Council of Canada (grant number 410-2004-1637).

References

Abrahamsen R and Williams M (2011) *Security beyond the State: Private Security in International Politics*. Cambridge: Cambridge University Press.

ASIS International (2013) *The United States Security Industry*. Alexandria, VA: ASIS International.

Avant D and Haufler V (2012) Transnational organizations and security. *Global Crime* 13(4): 254–275.

Ayling J, Grabosky P and Shearing C (2008) *Lengthening the Arm of the Law: Enhancing Police Resources in the Twenty-First Century*. Cambridge: Cambridge University Press.

Bartel A (1975) An analysis of firm demand for protection against crime. *Journal of Legal Studies* 4(2): 443–478.

Bartrip PWJ and Fenn PT (1983) The evolution of regulatory style in the nineteenth century British factory inspectorate. *Journal of Law and Society* 10(2): 201–222.

Bayley D and Shearing C (2001) *The New Structure of Policing: Description, Conceptualization and Research Agenda*. Washington, DC: National Institute of Justice.

Becker G (1974) Crime and punishment: An economic approach. In: Becker G and Landes W (eds) *Essays in the Economics of Crime and Punishment*. Cambridge: National Bureau of Economic Research.

Bellot C and Cousineau MM (1996) Le metro: Espace de vie, espace de contrôle. *Déviance et Société* 20(4): 377–395.

Berg J (2010) Seeing like private security: Evolving mentalities of public space protection in South Africa. *Criminology and Criminal Justice* 10(3): 287–301.

Boyd N (1995) Violence in the workplace in British Columbia: A preliminary investigation. *Canadian Journal of Criminology* 37(4): 491–519.

Brodeur J-P (2010) *The Policing Web*. Oxford: Oxford University Press.

Button M (2007) Assessing the regulation of private security across Europe. *European Journal of Criminology* 4(1): 109–128.

Button M (2008) *Doing Security: Critical Reflections and an Agenda for Change*. Basingstoke: Palgrave Macmillan.

Castillo DN and Jenkins L (1994) Industries and occupations at high risk for work-related homicide. *Journal of Occupational and Environmental Medicine* 36(2): 125–132.

Clotfelter C (1978) Private security and the public safety. *Journal of Urban Economics* 5(3): 388–402.

Cook P and MacDonald J (2011) Public safety through private action: An economic assessment of BIDS. *The Economic Journal* 121(552): 445–462.

Crawford D (2009) Deutsche Bank spy case rises to new levels. *The Wall Street Journal*, 9 October, C2.

Cunningham W, Strauchs J and Van Meter C (1990) *Private Security Trends 1970 to 1990: The Hallcrest Report II*. Boston, MA: Butterworth-Heinemann.

Cusson M and Diotte ME (2007) Les organismes de sécurité intérieure au Québec: Une classification. In: Cusson M, Dupont B and Lemieux F (eds) *Traité de sécurité intérieure*. Montréal: HMH Hurtubise, pp. 89–97.

Darlin D (2006) Deeper spying is seen in Hewlett Review. *New York Times*, 18 September, A1.

Datamonitor (2011) *Global Security Services*. New York: Datamonitor.

Davis R, Ortiz C, Dadush S, et al. (2003) The public accountability of private police: Lessons from New York, Johannesburg, and Mexico City. *Policing and Society* 13(2): 197–210.

De Pierrebourg F and Noël A (2011) Sous la loupe des enquêteurs, l'ex-chef de police. *La Presse*, 12 April, A2.

De Waard J (1999) The private security industry in international perspective. *European Journal on Criminal Policy and Research* 7(2): 143–174.

Ditton J (1977) Perks, pilferage, and the fiddle: The historical structure of invisible wages. *Theory and Society* 4(1): 39–71.

Dupont B (2004) Security in the age of networks. *Policing and Society* 14(1): 76–91.

Dupont B (2006) Delivering security through networks: Surveying the relational landscape of security managers in an urban setting. *Crime, Law and Social Change* 45(3): 165–184.

Economist, The (2009) Nuclear conflict: Did EDF, France's nuclear-energy giant, spy on Greenpeace? *The Economist* 390(8628): 67.

Evans D and Schmalensee R (2005) *Paying with Plastic: The Digital Revolution in Buying and Borrowing*. Cambridge, MA: MIT Press.

Favarel-Garrigues G, Godefroy T and Lascoumes P (2008) Sentinels in the banking industry: Private actors and the fight against money laundering in France. *British Journal of Criminology* 48(1): 1–19.

Friedman J, Hakim S and Spiegel U (1987) The effects of community size on the mix of private and public use of security services. *Journal of Urban Economics* 22(2): 230–241.

Gill M and Hart J (1999) Enforcing corporate security policy using private investigators. *European Journal on Criminal Policy and Research* 7(2): 245–261.

Gill M and Taylor G (2004) Preventing money laundering or obstructing business? Financial companies' perspective on 'know your customer' procedures. *British Journal of Criminology* 44(4): 582–594.

Graham C and Shirm S (1995) Security in pediatric emergency departments. *Pediatric Emergency Care* 11(4): 220–222.

Hobbs D, Hadfield P, Lister S, et al. (2003) *Bouncers: Violence and Governance in the Night-Time Economy*. Oxford: Oxford University Press.

Huey L, Ericson R and Haggerty K (2005) Policing fantasy city. In: Cooley D (ed.) *Re-Imagining Policing in Canada*. Toronto: University of Toronto Press, pp. 140–208.

Johnston L (1999) Private policing in context. *European Journal on Criminal Policy and Research* 7(2): 175–196.

Johnston L and Shearing C (2003) *Governing Security: Explorations in Policing and Justice*. London: Routledge.

Jones T and Newburn T (1998) *Private Security and Public Policing*. Oxford: Oxford University Press.

Kempa M and Singh AM (2008) Private security, political economy and the policing of race: Probing global hypotheses through the case of South Africa. *Theoretical Criminology* 12(3): 333–354.

Kempa M, Stenning P and Wood J (2004) Policing communal spaces: A reconfiguration of the 'mass private property' hypothesis. *British Journal of Criminology* 44(4): 562–581.

Kraus JF (1987) Homicide while at work: Persons, industries, and occupations at high risk. *American Journal of Public Health* 77(10): 1285–1289.

Lippert R, Walby K and Steckle R (2013) Multiplicities of corporate security: Identifying emerging types, trends and issues. *Security Journal* 26(3): 206–221.

Loader I and Walker N (2006) Necessary virtues: The legitimate place of the state in the production of security. In: Wood J and Dupont B (eds) *Democracy, Society and the Governance of Security*. Cambridge: Cambridge University Press, pp. 165–195.

Loader I and Walker N (2007) *Civilizing Security*. Cambridge: Cambridge University Press.

Manning P (2006) Two case studies of American anti-terrorism. In: Wood J and Dupont B (eds) *Democracy, Society and the Governance of Security*. Cambridge: Cambridge University Press, pp. 52–85.

MarketLine (2013) *Global Security Services*. London: Informa.

Marks M and Wood J (2007) The South African policing 'nexus': Charting the policing landscape in Durban. *South African Review of Sociology* 38(2): 134–160.

Mazerolle L and Ransley J (2005) *Third Party Policing*. Cambridge: Cambridge University Press.

NACCJG (National Advisory Committee on Criminal Justice Standards and Goals) (1976) *Report of the Task Force on Private Security*. Washington, DC: National Institute of Justice.

Nalla M and Newman G (1990) *A Primer in Private Security*. New York: Harrow and Heston.

Nasheri H (2005) *Economic Espionage and Industrial Spying*. Cambridge: Cambridge University Press.

O'Connor D, Lippert R, Spencer D, et al. (2008) Seeing private security like a state. *Criminology and Criminal Justice* 8(2): 203–226.

Ocqueteau F and Dupont B (2013) Gérer les risques dans l'entreprise vulnérable: Une comparaison franco-québécoise. *Criminologie* 46(2): 171–193.

Ocqueteau F and Pottier ML (1995) *Vigilance et sécurité dans les grandes surfaces*. Paris: L'Harmattan.

O'Malley P and Hutchinson S (2007) A genealogy of 'fire prevention'. In: Brannigan A and Pavlich G (eds) *Governance and Regulation in Social Life: Essays in Honour of W. G. Carson*. New York: Routledge-Cavendish, pp. 145–163.

O'Reilly C (2011) From kidnaps to contagious diseases: Elite rescue and the strategic expansion of the transnational security consultancy industry. *International Political Sociology* 5(2): 178–197.

Permanent Subcommittee on Investigations (2008) *Tax Haven Banks and U.S. Tax Compliance*. Washington, DC: United States Senate.

Prenzler T and Sarre R (2008) Developing a risk profile and model regulatory system for the security industry. *Security Journal* 21(4): 264–277.

Rigakos G (2002) *The New Parapolice: Risk Markets and Commodified Social Control*. Toronto: University of Toronto Press.

Rigakos G (2005) Beyond public–private: Towards a new typology of policing. In: Cooley D (ed.) *Re-Imagining Policing in Canada*. Toronto: University of Toronto Press, pp. 260–319.

Rochet JC and Tirole J (2006) Two-sided markets: A progress report. *RAND Journal of Economics* 37(3): 645–667.

Shearing C and Stenning P (1981) Modern private security: Its growth and implications. In: Tonry M and Morris N (eds) *Crime and Justice: An Annual Review of Research*. Chicago, IL: University of Chicago Press, pp. 193–245.

Shearing C and Stenning P (1983) Private security: Implications for social control. *Social Problems* 30(5): 493–506.

Shearing C and Stenning P (1987) Say ‘Cheese!’: The Disney order that is not so Mickey Mouse. In: Shearing C and Stenning P (eds) *Private Policing*. Los Angeles, CA: SAGE, pp. 317–323.

Shearing C and Wood J (2003) Nodal governance, democracy and the new ‘denizens’. *Jounal of Law and Society* 30(3): 400–419.

Shields M and Wilkins K (2006) *Findings from the 2005 National Survey of the Work and Health of Nurses*. Ottawa: Statistics Canada.

Sims B (2010) MBD forecasts annual growth between 2%–4% for UK guarding to 2015. *IFSEC Global*, 3 September. Available at: http://www.ifsecglobal.com/document.asp?doc_id=551929 (last accessed 7 December 2013).

South N (1988) *Policing for Profit: The Private Security Sector*. London: SAGE.

Spitzer S and Scull A (1977) Privatization and capitalist development: The case of the private police. *Social Problems* 25(1): 18–29.

Stenning P (2000) Powers and accountability of private police. *European Journal on Criminal Policy and Research* 8(3): 325–352.

Valverde M (2010) Questions of security: A framework for research. *Theoretical Criminology* 15(1): 3–22.

Van Duyne P (1993) Organized crime and business crime-enterprises in the Netherlands. *Crime, Law and Social Change* 19(2): 103–142.

Van Steden R (2007) *Privatizing Policing: Describing and Explaining the Growth of Private Security in the Netherlands*. The Hague: Boom Legal.

Van Steden R and Sarre R (2007) The growth of private security: Trends in the European Union. *Security Journal* 20(4): 222–235.

Wakefield A (2003) *Selling Security: The Private Policing of Public Space*. Cullompton: Willan Publishing.

Weiss R (1987) From ‘slugging detectives’ to ‘labor relations’: Policing labor at Ford, 1930–1947. In: Shearing C and Stenning P (eds) *Private Policing*. Los Angeles, CA: SAGE, pp. 110–130.

White A (2010) *The Politics of Private Security: Regulation, Reform and Re-Legitimation*. Basingstoke: Palgrave Macmillan.

White A (2011) The new political economy of private security. *Theoretical Criminology* 16(1): 85–101.

Williams JW (2005) Reflections on the private versus public policing of economic crime. *British Journal of Criminology* 45(3): 316–339.

Wood J and Shearing C (2007) *Imagining Security*. Cullompton: Willan Publishing.

Zedner L (2009) *Security*. New York: Routledge.

Author biography

Benoit Dupont is professor of criminology at the Université de Montréal, where he holds the Canada research chair in Security and technology. He is also the Director of the International Centre for Comparative Criminology. His research interests focus on the governance of security and the use of networked initiatives to enhance offline and online safety, as well as the coevolution of crime and technology.