Special Issue on The Global Governance of Security and Finance

SECURITY DIALOGUE

Reluctant partners? Banks in the fight against money laundering and terrorism financing in France

Security Dialogue
42(2) 179–196
© The Author(s) 2011
Reprints and permission: sagepub.co.uk/journalsPermissions.nav
DOI: 10.1177/0967010611399615
sdi.sagepub.com
SAGE

Gilles Favarel-Garrigues
CNRS, Sciences Po/CERI, France

Thierry Godefroy
CNRS, CESDIP, France

Pierre Lascoumes
CNRS, Sciences Po/CEE, France

Abstract

The implementation of the ongoing anti-money laundering/counter-terrorism financing (AML/CTF) drive within the private sector reflects a tension between the logic of state sovereignty and that of neoliberal governmentality. In this article, we show that the main concrete output of two decades of global policy in this area is found in the routinization of professional interactions between banks and law enforcement agencies. Banks recruit former law enforcement officials and attempt to establish informal ties with the police or intelligence bodies. They are also actively involved in intelligence-led policing missions and have become embedded in interdependent relationships with law enforcement agencies. Drawing on data from 75 interviews conducted with AML/CTF professionals within France, the article shows how new everyday professional routines in the banking sector reflect governmentality in the making.

Keywords

policing, surveillance, money laundering, international security, banks, Foucault, governmentality

Introduction

The development of the fight against 'dirty money' at the international level since 1989 gave rise to little research over the course of the 1990s, with the exception of the interest shown by some criminologists, jurists and international relations scholars (e.g. Levi, 1991; Naylor, 1997; Van Duyne, 1998; Helleiner, 1999; Sheptycki, 2000). This situation changed after 9/11, however, when

Corresponding author:
Gilles Favarel-Garrigues
Email: faverel@ceri-sciences-po.org

the Bush administration declared a 'war on terror' that would include a significant financial component (Amoore and De Goede, 2008b; Biersteker and Eckert, 2007; Naylor, 2006). The fight against terrorism financing has been assigned to institutions that had previously specialized in anti-money laundering activities. The latter have drawn on methods and expertise already developed in the 'war on drugs' and efforts to combat organized crime (Heng and McDonagh, 2009), and since 9/11 the surveillance of financial flows has seen considerable growth.

Efforts to tackle 'dirty money' rely on cooperation between law enforcement and various financial professions, and involve a way of governing that betrays the existence of a tension between the conflicting logics of state sovereignty and 'neoliberal governmentality' (Amoore and De Goede, 2008a). Governmentality includes a series of surveillance practices carried out by the banking industry, though these have been the subject of little academic study (Harvey, 2004, 2008; Yeandle et al., 2005; Canhoto, 2007; Verhage, 2009). Our objective here is to explore the everyday consequences of the global drive against 'dirty money'. To do this, we have carried out a sociological study in French banks, interviewing compliance officers whose duties include responsibility for anti-money laundering/counter-terrorist finance (AML/CTF) activities (Favarel-Garrigues et al., 2008). First, then, how does observation of surveillance practices in banks help to understand neoliberal governmentality in the making?

The financial professions were not predestined for the role of identifying and managing suspicious transactions. Indeed, bankers are known to have developed a professional culture of non-interference in the financial operations of their clients and strict respect for confidentiality. For this reason, they are often suspected of faking commitment in their involvement in AML/CTF activities. However, financial surveillance has become a daily routine for banking actors (Levi and Wall, 2004) and is now part of the broader surveillance dynamics described by Lyon (2003, 2006). In order to conduct such surveillance, banks have invested in watch lists and software-based profiling tools, and have developed a range of practical guidelines to regulate their use. Relying on these instruments, compliance officers decide whether particular customers should be included in or excluded from banking operations (Gandy, 2006; Martin, 2007).

Through a focus on the views and activities of compliance officers, we aim to show that financial surveillance is not only causing intra-organizational effects within the financial sector but also fostering the development of unanticipated professional interactions between the milieus of banking and law enforcement. In our view, the routinization of interpersonal exchanges of information between these milieus has been the most important consequence of the implementation of anti-money laundering standards. Cooperation between these distinct professional worlds has become institutionalized. Banks recruit former police officers and judges, respond to solicitations from government agencies and, when necessary, unofficially approach public authorities for information they require to help them assess situations they believe may involve risk. New routines foster 'intelligence gathering' (McCue, 2006; Gelemerova, 2009) or 'joined-up intelligence' work (Yeandle et al., 2005). It is not limited to official channels for the submission of suspicious activity reports (SARs) to national financial intelligence units (FIUs), but manifests itself in the form of more or less formalized multiple interactions. In the French context, such practices are all the more unexpected in that the AML/CTF policy had been designed to establish a 'Great Wall' between the banks and the police. In contrast to the situation in other countries, France's financial intelligence unit, Tracfin, is a part of the country's ministry of finance, acting as an intermediary between the financial world and law enforcement institutions.

The research presented in this article is part of a wider project to compare the implementation of AML/CTF policy by professionals in France and Switzerland (Favarel-Garrigues et al., 2009). Most of the data it draws on are taken from the professional literature and interview material.

In total, 75 interviews were conducted in two stages between 2005 and 2008 with chief compliance officers at banks' headquarters and their regional counterparts. The study was complemented by interviews with law enforcement personnel, Banking Commission personnel,[1] Tracfin agents, officials from France's data protection authority (CNIL) and software providers.

The article is divided into three parts. In the first, we discuss how the AML/CTF drive reflects a tension between the logic of state sovereignty and that of neoliberal governmentality, showing how the analysis of the everyday practices of banking surveillance may help to understand this tension. In the second, we describe formal and informal relationships between compliance officers and FIU officials, and in the third we examine information swaps between bankers and police officials and other intelligence providers.

Is there a prince in the tower? The AML/CTF drive between state sovereignty and governmentality

On one hand, the ongoing AML/CTF drive is often considered an issue of state sovereignty, as it is based on a 'pre-emptive intervention of state institutions' (Vlcek, 2008). Although the fight against terrorism financing is a non-military component of the 'war on terror' (Heng and McDonagh, 2009), it has nevertheless been connected to the need to respond to the possibility of imminent attack: 'Our security will be required ... to be forward looking ... to be ready for pre-emptive action when necessary.... We must uncover terrorist cells in 60 or more countries using every tool of finance, intelligence and law enforcement' (Bush, 2002). The issue of sovereignty is underlined by analyses that, from an Agambenian perspective, emphasize the exceptionalism of the 'war on terror' (Aradau and Van Munster, 2009). The financial component of this 'war' is associated with a set of 'pre-emptive security' measures that normalize suspicion and tend to include or exclude players from international financial flows (Martin, 2007). Managing situations that are highly uncertain, these measures reflect sovereign decisions in the sense that they are presented as urgent and technical measures, and therefore not to be submitted to political debate (Aradau and Van Munster, 2008a,b).

On the other hand, the fight against money laundering also pertains to a form of governmentality. It is based on governmental requirements that seek to define the norms according to which private actors are to act, but where questions relating to how those norms are to be concretely implemented are delegated to the actors themselves. The AML/CTF drive was operationalized by national legislation and European directives that regulate the relationship between bankers and their clients in new ways. The originality of these apparatuses lies in their introduction of the state into the surveillance of what had previously been a strictly private interaction, regulated by contractual relations of confidentiality and non-intervention. This is indeed the realization of 'governmentality at distance' and converges with how Foucault conceived power, not as a possession that is conquered or that one appropriates, but as a relationship, a series of continuous interactions between an authority (a governing entity) and subjects (the governed). In order to describe this type of discipline, Foucault resorted to the metaphor of the Panopticon, which allowed him to conceptualize power without 'the prince'. This type of disciplinary power is not based on the existence of a central authority,[2] but is 'the result of techniques, practices and relationships of force with populations' (Foucault, 1976: 128). The way in which the AML/CTF fight has been implemented has not involved the granting of a series of powers of control and punishment to a public entity, but has rather been based on a strong push for the interiorization of discipline within the private sector, under the supervision of a state agency. This process of making private economic actors responsible is a manifestation of the diffusion of techniques of power (De Goede, 2007a,b). As De Goede

has pointed out, Butler's concept of 'petty sovereigns' is relevant for analysing the role of banks in the AML/CTF drive. Having been forced by the government to carry out a law enforcement role, financial institutions now act as 'petty sovereigns', deciding for instance whether to include or exclude particular customers (for a discussion of the relationships between 'petty sovereigns' and governmentality, see Epstein, 2007: 161). According to Butler (2004: 65), 'petty sovereigns' do not know

> about what work they do, but perform their acts unilaterally and with enormous consequences. Their acts are clearly conditioned, but their acts are judgments that are nevertheless unconditional in the sense that they are final, not subject to review, and not subject to appeal.

In practice, banks have translated governmental requirements into a set of risk-management measures. They have purchased computing technologies, hired professionals, and set internal norms and procedures in order to manage financial and penal risks. Indeed, the AML/CTF drive itself pertains less to a logic of precaution (Aradau and Van Munster, 2008b: 30), which would assume a radical uncertainty, not objectified and not probabilized (O'Riordan and Cameron, 1994; Freestone and Hey, 1996; Callon et al., 2009: 191–223), than to a logic of risk management. Moreover, the transformation of AML/CTF policy into risk management was produced within the banks through the extension of control apparatuses that were already being used to address other issues (e.g. the commission of fraud against banks). After a first phase of resistance (1990–2001), France's private financial actors integrated anti-money laundering measures, translating them into management of 'operational risks' (Power, 2003, 2007; Jobst, 2007). As a process designed to identify potential events that might adversely affect a bank's interests, risk management 'is a form of self-insurance in its own right, and self-insurance provides incentives to invest in control systems' (Power, 2004: 27). Implementing AML/CTF software accords with a strategy of 'defendable compliance' by which banks cover themselves with respect to regulators. As Ericson (2006: 346) puts it: 'Risk managers facing an increasingly litigious environment for failures become defensive, focusing more on operational risks that might affect the reputation of their organization than on the real risks they are supposed to manage.'

The development of a risk-based AML/CTF approach within the banks was facilitated by the negotiations of the Basel II agreements, which entrusted bankers with the responsibility to evaluate by themselves the risks they face (Gallati, 2003; Pradier, 2006). The approach was also promoted by the Financial Action Task Force (FATF),[3] which has called on financial actors to adopt 'a risk management process for dealing with money laundering and terrorism financing. This process includes recognizing the existence of the risk(s), undertaking an assessment of the risk(s) and developing strategies to manage and mitigate the identified risks' (see FATF-GAFI, 2007: 7). The obligation to analyse transactions according to specific countries/geographical areas, customers, benefits, financial products or transaction purposes was a strong driver behind the development of risk-assessment tools. Software companies and private international consulting firms began to take an interest in AML/CTF implementation, while on the other side compliance officers devoted considerable time and effort to choosing, coordinating and disseminating AML/CTF software tools.

However, the adoption of such an approach in the 'war on terror' has been criticized in some quarters because it engenders a certain naturalization of risks by focusing upon transnational mobilizations (Beck, 2002; Rasmussen, 2006; Mythen and Walklate, 2006). Within such a critical perspective, risk should be seen 'as an instrument of governance rather than an organizing principle of life' (c.a.s.e collective, 2006: 468; see also Aradau and Van Munster, 2008a,b). Such a conception

of risk management meets Holzer and Millo's (2005) analysis of risk construction, which relates to decisionmaking in a situation of uncertainty. According to the latter authors, uncertainty cannot always be fully reduced, but it nevertheless does not rule out the need for a decision. If probabilistic assessment can justify taking some risk, it does not always provide enough grounds on which to base a decision, as AML/CTF risks managed by compliance officers show. These risks can generate costs (financial, legal and reputational), but they are partially controllable through diligent actions. Justified decisions remain based upon a limited rationality, but two factors contribute to the choices made: the available technological resources (here, computer resources) and the internal organization of AML/CTF risk-management departments (hierarchical distribution of skills). Both are conceived of as decisionmaking support systems. In this sense, they contribute to the construction of risk. 'Technology and bureaucratic organisation take part in an intertwined process through which a world of dangers is transformed into a world of risks' (Holzer and Millo, 2005: 5).

In Foucault's ([1978] 1994: 637–57) concept of 'governmentality', the characterization of the liberal regime of power is based on material practices and not on the regime's intentions or the discourses it uses to legitimize itself. Such an approach implies that

> we place at the heart of the analysis neither the general principle of the law nor the myth of power, but the multiple and complex practices of 'governmentality' that assume, on the one hand, rational forms, technical procedures, instrumentalities through which governmentality is exercised and, on the other hand, strategic stakes that render unstable and reversible the relations of power they are supposed to secure.

As Dean (1999: 28) has summarized, with the concept of governmentality 'the priority (is) given to "how" questions'. In Dean's (1999: 21) view, Foucault 'considers how this regime has a technical or technological dimension and analyses the characteristic techniques, instrumentalities and mechanisms through which such practices operate, by which they attempt to realize their goals, and through which they have a range of effects'. This is why analysis of the AML/CTF drive's risk management must not be limited to the study of institutional discourses, but must also rely upon observation of the daily practices of those who are responsible for AML/CTF functions (for a similar approach in relation to global finance, see Langley, 2009). Such an approach allows us to observe in a practical way the diffusion and appropriation of a new governmental technique that enables the normative guidance of banking activities from a distance. The discipline expected from the anti-money laundering apparatus is only superficially based on sanctions, as it also comes from the appropriation and translation (Callon, 1986) of legal and professional norms by financial actors. How do compliance officers give AML/CTF norms a meaning in terms of the operationalization of which customers and transactions are seen as normal and deviant? How do they integrate AML/CTF norms into their organizations' internal risk-management policies? Their behaviour is determined not only by pressure or fear of punishment, but also by the strategic games they play in interpreting or resisting those norms.

In order to satisfy legal requirements, banks have implemented continuous and automated protective systems that evaluate emerging risks and classify them within a hierarchy of importance. From then on, seeing money laundering in terms of operational risk, they do not stop at identifying offenders on the basis of their financial activities. They have implemented monitoring systems that seek to identify both potential upstream threats and suspicious profiles and behaviours. To assist them in cases where they are in doubt, they have also attempted to establish close connections with various intelligence and law enforcement bodies. The perceived need for data exchange with these actors is a result of the increasing importance of risk-management strategies and technologies within the banks themselves.

Routine relations between banks and France's financial intelligence unit

While the current drive against money laundering was launched in 1989, its implementation within France's banking sector began only in the early 2000s through a convergence in agendas related to international (the impact of the post-9/11 'war on terror') and national crises (the indictment for money laundering of senior managers at two leading banking and insurance companies, Société Générale and AXA).

France's AML/CTF legislation specifies that banks have a mandatory responsibility to report any suspicions they may have about particular customers or transactions to a national financial intelligence unit (FIU). In France, this organization is known as Tracfin, and in this section we describe the ways in which the French banking sector interacts with Tracfin. Are they 'partners', as is often assumed in relation to cases of public–private policing, even in the context of financial institutions (Edwards and Wolfe, 2006)? Is the AML/CTF regime an example of the 'reliance of contemporary regulatory regimes upon hybrid models of public–private partnership' (Zedner, 2006: 282)? Through our survey, we have analysed how compliance officers deal with the surveillance of customers and financial transactions on an everyday basis. How do they address cases where they have doubts? How do they 'target and stay on the targets' (Hornqvist, 2010: 28–64)?

The routine activity of compliance officers' relationships with Tracfin is exemplified in the filing of a suspicious activity report (SAR), an act that may trigger judicial proceedings. Before submitting such a report, a compliance officer must have analysed computer alerts, expressed doubts about particular individuals or transactions, and finally translated these doubts into more concrete suspicions. Only once these things have been done is a case reported to the FIU (in the case of about one out of every 10,000 computer alerts, according to our survey). Since 2002, 74,000 SARs have reached Tracfin. In response to the around 12,000 reports that are received annually, Tracfin undertakes about 1,000 preliminary investigations that give rise to 600 full investigations, which in turn lead to the referral of around 400 cases to the courts. Tracfin thus acts as a complainant: it is a triggering element. Carrying out such a function within the judicial system constitutes Tracfin's front mission and main performance indicator, and serves to keep its intelligence activity in the background: 'In Paris, three-quarters of the money-laundering cases start with a Tracfin tip. The number of SARs referred to the courts has grown: it reached 407 dossiers in 2005' (Interview 40). This is how Tracfin can claim to have an intermediary position 'between professional practices and law enforcement, with an intelligence component' (Interview 40). The institution then aims to 'relay civil society participation to penal policy by making cooperation of financial actors obligatory' (Interview 40).

On the whole, compliance officers have responded by cooperating with this obligation to report, but their behaviour is nevertheless ambiguous. In practice, they resort simultaneously to subversive tactics, harsh criticism and pragmatic behaviour in their attempts to decipher Tracfin's expectations.

Reporting suspicion

The practice of 'defensive filing' or 'umbrella reports', which involves 'reporting everything', has been associated with a phenomenon of 'overcompliance' (Gelemerova, 2009: 53). It has also been suggested that compliance officers are just 'doing enough to proverbially "cover their backs"'

(Harvey and Fung Lau, 2009: 70), even if they deny a simple 'cover your ass' policy (Verhage, 2009: 30; see also Harvey, 2004; Levi, 2007). Such defensive practices would amount to a subversive form of disobedience, acting as a way of sabotaging the system, intentionally or otherwise, by swamping Tracfin with cases requiring attention. 'The only way to cover yourself is to file a suspicious activity report for each case that arises.... That is because the legislation is poorly written. And too bad if Tracfin faces unmanageable flows' (Interview 5). Reluctance to cooperate can also be seen in the vocabulary used by some of our respondents, for whom 'notifying Tracfin' boiled down to 'turning a customer in to the authorities' (Interview 35). Some justified their 'overcompliance' by referring to the contradictory nature of the requirements specified by Tracfin and the Banking Commission: 'Until 2004, Tracfin appreciated our being selective, but since then the Banking Commission has been pushing us to declare everything that is abnormal' (Interview 52). However, the flow of 'umbrella reports' has gradually been stemmed by Tracfin's determination to normalize the volume and content of SARs through the use of comparisons, benchmarking and dissemination of good practices. In every year since 2004, Tracfin has received a stable number of SARs. In relation to counter-terrorism financing, most compliance officers have been surprised by the sparse results of the 'war on terror' since 9/11: 'We have reported about 20 terrorism-financing cases: just bullshit that has scared us for nothing' (Interview 29). Some, on the other hand, imagine that they are actually dealing with dangerous terrorists and do not understand why Tracfin has neglected their reports:

> When you see how much is spent on AML/CTF, it makes you furious with the administration. I and my co-workers often feel a lot of frustration: we send rock-solid dossiers to Tracfin on terrorism financing and nothing happens. On the other hand, we would have got our hand slapped if we let the case go by. They don't back us up. (Interview 58)

Most of the bank officials interviewed suggested that Tracfin was understaffed and incompetent.

Cooperation with Tracfin is ultimately obligatory, but its expectations appear to be difficult to decode. Compliance officers have trouble understanding what kinds of reports Tracfin is interested in, and complain about the lack of feedback from the FIU in relation to the suspicious activity reports they do file. They also would like to have more personal contacts with Tracfin representatives:

> We meet them about once a year, [when] we go over our suspicious activity reports. And this is the only time when we get a little feedback on some cases. They tell us that when reports that we file involve less than €50,000,[4] they're filed away immediately. The most difficult part is making up our minds as to whether it is a fiscal matter or not. (Interview 52)

According to another respondent, Tracfin's decisions reflect a practical prioritization of cases. Even if the FIU is obliged to record all the suspicious activity reports it receives, there are implicit rules of classification:

> When a suspicious activity report reaches Tracfin, I think they make three piles: The first one includes cases below €50,000 and they don't even look at it; the second one includes cases involving customers who are already in their files, and then they have a look; the third one contains well-documented cases, which are either filed away or kept on the table, depending on how much time they consider they'll have to spend to find something. (Interview 56)

Moreover, each Tracfin agent sets his or her own priorities:

> We just met our third Tracfin correspondent. Whereas the first was interested in small narcotics trafficking, which meant that we filed a lot of SARs, the second only wanted big cases, which are cases that involve sums of over €150,000 and that would attract media attention. (Interview 56)

Tracfin officials claim that collecting sensitive information that is not necessarily immediately useful and where the origin of the supposedly laundered capital is not yet known is part of the organization's mission. They store such data and relay details to other governmental intelligence bodies when necessary. Tracfin's discretionary powers in relation to the collection and transmission of intelligence result in incoherent action and priorities that are not clear to the organization's correspondents within the banks. However, difficulties in discerning Tracfin's objectives stem from a misperception of the institution: compliance officers tend to view the FIU as a link in the criminal chain, and interpret its demands in the light of such an understanding, whereas Tracfin is basically an intelligence service. Bank compliance officers who had clearly identified Tracfin as an intelligence unit were far less surprised at the small volume of cases transmitted to the judicial authorities.

Reluctant partners?

Tracfin personnel seem wary of bank staff, suspecting them of wanting to substitute arbitrary alerts and routine checklists for the ability to make a judgement: 'They argue in favour of automatic reports and blacklists because they don't want to be held responsible for their decisions' (Interview 9). Such beliefs relate to the contents of the suspicious activity reports that are transmitted to the FIU: 'Bankers know very well the difference between a real report and a mere desire to cover themselves. As regards SARs, the law mentions the bankers' "good faith", which constitutes a warning to them' (Interview 40).

Tracfin has thus set out to clarify its expectations towards compliance officers: 'We invite them to act as an intelligent cog in the wheel' (Interview 68). In relation to the objectives of the fight against money laundering, this task is made easier by the fact that it involves demonstrating a certain convergence of interests. Tracfin officials in fact reiterate that their institution was set up mainly to fight serious crime, and the fact that in practice this objective is not achieved provokes a certain degree of frustration: 'We do a good job with regard to average-to-serious crime, but we need to do better regarding big money launderers. These crimes are well concealed by legitimate economic activities, and thus hard to catch with AML/CTF tools' (Interview 68).

On the other hand, Tracfin officials are reluctant to deal with petty tax fraud and express this in terms similar to those used by compliance officers:

> We're concerned with tax fraud, but we want to preserve our mechanism [that of a FIU] and its purpose. The anti-money laundering efforts should deal with serious violations and not petty tax fraud. Our job is not to go after the local baker. That would be counterproductive and stupid, even if organized fraud exists. When you're working on major fraud, on organized crime, you want your efforts to pay off. (Interview 40)

Tracfin's activity is based on one of the founding principles of AML activities, that of the existence of a 'Great Wall of China' between AML intelligence services and the revenue service, even if there seem to be ways of bypassing that divide. Already observed at the international level in relation to the activities of the FATF, the principle of differentiated management of small tax

violations and serious crime constitutes one of the foundations of the fight against money laundering because it ensures at least a minimum of cooperation from banks.

The existence of a broad consensus on AML policy does not eliminate all ambiguities in its implementation, particularly in relation to the content of suspicious activity reports. Tracfin insists that it does not intervene in the drafting of suspicious activity reports. In any event, its officials suggest that it would be impossible to formulate 'a single set of guidelines': there is no doctrine concerning the optimum number of reports that banking institutions should file. Indeed, very similar banks have very different practices: 'The number of reports can vary between 100 and 500 for leaders in the banking sector. There's no single rule, no model' (Interview 68). Delegating the AML/CTF mission to financial actors is justified by reference to the heterogeneous activity of banking establishments.

Tracfin nevertheless is trying to increase the volume of more or less formalized exchanges between its officials and compliance officers. Within the FIU, some agents have been appointed to act as regional contacts. Investigators work independently and are encouraged to 'go fishing for information and call their correspondents' (Interview 68). Moreover, Tracfin encourages compliance officers to develop routine interpersonal relations with their correspondents in the FIU.

Finally, Tracfin agents promote informal meetings with bankers and compliance officers in order to clarify their expectations. During such meetings, we have observed that the 'partnership' between Tracfin and the banks suffers from low levels of mutual trust. As one Tracfin official said during one of these meetings:

> Report everything, but let us know if you believe there are real grounds for suspicion or if the information is just to cover yourselves. Invent a little code to tell us that it is not a real suspicion.

By suggesting practices like this, Tracfin is seeking to convince the banks that such an approach will enable them to satisfy both the FIU's requirements and those of the Banking Commission. According to the same official, 'We have to record everything. The SAR remains in a database that can be reactivated, and the reporting party will be protected from the Banking Commission without creating a bottleneck for Tracfin.' These efforts to frame relations aim to give Tracfin the image not of a body that censors but of one that works in partnership, allowing private institutions the 'right to make mistakes', even to have 'occasional failures', according to an interview with one Tracfin agent (Interview 68). However, from the banks' point of view, discrepancies between Tracfin's expectations and those of the Banking Commission appear to constitute a double bind.

In practice, informal interactions between the banks and Tracfin are more or less developed. In some banks, they have existed for a long time. In these cases, respondents point out that they are in regular contact with Tracfin and that they even know when one of their suspicious activity reports has been referred to the judiciary. Most of them just respond to Tracfin's inquiries, but some respondents claim an ability to anticipate Tracfin initiatives and thus make contact themselves: 'Sometimes Tracfin calls me, but it's usually me who calls them about current cases about which I can't manage to form an opinion. I ask, "Does this name mean anything to you?"' (Interview 46).

Others do not use Tracfin as a source of information about their customers because they seem unable to access this type of service:

> Tracfin receives information but doesn't give any out.... What I'm looking for is an exchange. If only I was able to call Tracfin to find out if they have a record of such and such a customer or not.... We sometimes get an answer, but it doesn't come naturally. (Interview 47)

The lack of contact can also be explained by reference to a desire to privilege other information channels, particularly banks' networks of counterparts in other banks, a subject to which we shall return later. For compliance officers who are reluctant to cooperate with law enforcement agencies, Tracfin and the police are part of the same universe. In particular, they denounce the tendency of the FIU to reveal confidential information, just as the police do, thereby heightening the antagonism between the banking and law enforcement professions and acting in a way that runs counter to the banking milieu's respect for confidentiality. Although an online reporting system has been implemented that conceals the identity of an individual submitting an SAR behind a user code, banks still worry about the consequences they might face in terms of civil liability if an exposed customer decides to sue them. This wariness is heightened by the length of time Tracfin keeps information on file (ten years).[5]

Our survey shows that relations of trust between the banks and Tracfin are difficult to build. In practice, relations are based on mutual illusory expectations, but they nevertheless create interdependence in terms of information exchange. On an everyday basis, then, the public–private partnership in the fight against money laundering and terrorism financing (Hardouin, 2009) remains marked by mutual wariness and its success should not be exaggerated. This is a partnership from Tracfin's point of view: indeed, among our interviewees, only Tracfin officials used this term to describe relations between the two sides. For compliance officers, describing their relationship with the FIU as a partnership would seem unwarranted.

To assist them to decide whether their doubts in particular cases should be converted into suspicions and reported, compliance officers seek to develop relations with potential partners (such as police officials) on the basis of information swaps, a subject to which we now turn.

Information swaps

The need for the intelligence required to back up the filing of a suspicious activity report leads to a multiplication of informal exchanges. Compliance officers often use their connections with counterparts in other banks or enter into relationships with private business intelligence firms. However, the most frequent information swaps occur between banks and the police, reflecting the development of new forms of intelligence-led policing (Ratcliffe, 2008).

Intelligence-gathering

While not every compliance officer in charge of AML/CTF duties will agree to perform intelligence-gathering tasks, some openly claim to perform such a function:

> We work as an intelligence unit: We do economic intelligence, exchange information.... People often think it's provocative to say that we are involved in intelligence! I say it to change mindsets: we have a real problem of professional culture! (Interview 1)

Some officials point out that the major banks already had intelligence units before the rise of AML/CTF policy, but that personnel in these units were recruited from specialized departments within the defence or interior ministries. Very often, the intelligence needs of banks only required filling a single position:

> I had 'my own SDECE',[6] an investigator and former member of the armed services who for a long time had done intelligence work on credit risks in the bank and is now actually involved in AML/CTF policy. (Interview 43)

The demand for financial surveillance has spurred the development of intelligence services in the private sector under the generic expression of 'business intelligence', a growing sector since the beginning of the 2000s. In France, however, the phenomenon remains fairly undeveloped, though a few initiatives have begun to emerge. This low trend is not only justified by the small total number of business intelligence firms established in France but also by the risks that these firms run in a country where state institutions intend to maintain their prerogatives in the intelligence realm. The activity of private firms is mainly related to foreign customers. As a staff member at one of these firms declared somewhat euphemistically: 'We mainly do cultural intermediation' (Interview 66).

The need for intelligence to back up suspicious activity reports has also led to multiplying informal exchanges among counterparts. Compliance officers often claim that they maintain cooperative relations among themselves regardless of the existence of any commercial competition among the institutions to which they belong. They often rely on 'colleagues with whom they are strongly tied for advice' (Mizruchi and Stearns, 2001: 667) when they need to make decisions on concrete cases. Thus, on behalf of those who are reluctant to do so, they provide an alternative to establishing unofficial relations with Tracfin or the police:

> I always work with my counterparts. I shouldn't say so, but we do it. I have contacts with other banking networks, and that works very well. If I have a doubt about a transaction or person, it's taken care of within the hour; for me, that's essential. It saves time and it's more efficient. (Interview 47)

As a general rule, compliance officers feel they can more easily get on the phone 'to their counterparts than to the Financial Crime or Intelligence Squad' (Interview 58); the same holds true in relation to Tracfin. Some compliance officers in Paris claim to be in contact with some 20 different counterparts (Interview 56).

Some networks are organized in such a way as to routinize the exchange of information:

> Outside of the monthly meetings organized by the French Banking Association AML committee with some fifteen major bank heads, I attend informal meetings of inspectors-general of major banking groups twice a year: we compare cases and tools. (Interview 5)

Participation in associations of specialized computer software users helps maintain social ties among compliance officers, who then share their questions and concerns, particularly regarding the practical use of lists of suspected terrorists and 'politically exposed persons' (PEPs) (Gilligan, 2009).

A few respondents resist the 'club' spirit that supposedly characterizes the anti-money laundering world – in other words, they find it difficult to reconcile themselves with the notion of setting aside competition among banks in order to establish a united front against 'dirty money'. Some compliance officers refuse to cooperate with counterparts who solicit their help. They believe that suspicious activity reports are one's own personal responsibility and require no external expertise:

> When I have doubts about a case, I never ask for an outside opinion. We can have exchanges about systems – there we're not in competition – but on cases I don't see the point. If I have a doubt, then I declare. (Interview 49)

Swapping information with the police

The issue of private–public exchanges within the broad context of crime control has been quite well documented as a form of 'plural policing' (see Dupont, 2011; Stenning, 2009; Wood and

Dupont, 2006) or as an example of the 'marketization' of control (see Zedner, 2006). However, in relation to the financial security sector, research remains scarce (Levi, 2003; Williams, 2005a,b). Looking at the ways in which AML/CTF policy has been implemented in practice may shed some light on exchanges that have been described as forms of a 'swap mode of security governance', 'characterized by a weak degree of constraint and a strong level of reciprocity between parties' (Dupont, 2011: 212).

These exchanges often rely on banks' own recruitment policies. With the 2001 momentum, the AML/CTF strategy has aggregated specialists from a range of different areas. Given the importance of the legal stakes – and in particular the dangers inherent in penal risks – banks have begun to recruit public officials, especially from law enforcement agencies and mainly from within their financial crime squads. Some banks had made a tradition of staffing their intelligence departments with former police officers, but recruitment practices changed in terms of both scope and quality when banks began to come under pressure. The new recruitments served three functions. First, banks demonstrated that they intended to obey the regulations in the course of their activities by resorting to 'undoubted guarantors of the law'. Next, people with the right sorts of CVs were sought after both for their personal networks and for their access to otherwise unavailable information: 'We see ex-police officers with very strong ties to their former colleagues.... What we were looking for with them is less the effectiveness of their AML fight than the access to their networks' (Interview 7). Finally, by serving as a communications interface with police and justice officials, these individuals could collect information about possible investigations and prepare the banks' defences in advance. These recruitments have met with harsh criticism within the banks, however, as the former officials are often viewed as outsiders.

Some compliance officers are reluctant to contact law enforcement agencies, but as a rule most banks attempt to foster access to police information. Most of the people we interviewed admitted that they maintained 'unofficial relations with the intelligence and police services' on a regular basis, through meetings and/or telephone contacts. Moreover, they believed that these exchanges have developed in tandem with the growth of the fight against terrorism financing. For compliance officers, such contacts are needed because they enable them to 'remove a doubt', 'confirm a suspicion' or 'put one's mind at ease about a big-time criminal' (Interview 1). From the banker's standpoint, these relations are often presented as an exchange of favours: 'If we see something unusual and we don't have any information, we can put the flows under surveillance, take a look at the context, ask the police for information. Their requests also help to corroborate our alerts' (Interview 52). Police intelligence helps in the creation of suspicious activity reports, while information from the banks feeds police investigations that are not necessarily related to cases of money laundering. The unofficial nature of these exchanges is explicitly highlighted in our respondents' statements:

> When there's a problem, we pick up the phone and go fishing for information, even if we can't use the information as such afterwards. In exchange, we give cops information about accounts when they need it, even if they aren't allowed to make official use of it either. Phone calls like this occur several times a week, especially for messy cases. Sometimes they say to us: 'Don't make your report right away. We're going to track them, give us 48 hours.' That puts us in an awkward position. (Interview 50)

Several interviewed compliance officers admitted that they had not expected that they would develop such relations with law enforcement agencies: 'One day the DST called me, I didn't want to call them back, I was terrified' (Interview 50). Such proximity entailed has also led some compliance officers to claim for themselves the role of police auxiliary:

> In fact, we've been transformed into police officers. We do investigations. We try to look at the flows, origins and destinations. To do so, we have unofficial relations with other banks and, if I really have a big doubt, with police contacts. In the latter case, those occur about once a month. (Interview 56)

The idea that the police use compliance officers by exploiting their fear of Banking Commission sanctions is sometimes expressed:

> The police try to keep the best cases for themselves. In some regions, police chiefs come to see banking professionals. They explain that Tracfin is far away and that they would do better to go directly to them. On the surface this is a respectable legal procedure, but behind the scenes people do things their own way. One of these days, a customer is bound to end up turning on the bank. (Interview 60)

As with Tracfin, the relations of compliance officers to law enforcement agencies are ambivalent. Wariness and criticism of the limits of police investment in anti-money laundering do not preclude the practical necessity of developing unofficial exchanges with police officials. Such exchanges, which are illegal but common, reflect a form of interdependence. As has been shown, the fraud squad needs banking expertise not only to keep an eye on a particular person or a company, but also to update its knowledge of the money launderers' *modi operandi* (Ericson, 2006). A 2008 initiative by the London police to recruit bankers to help combat financial crime in a country that leads both in financial services and in AML/CTF fight probably reflects a general tendency that France cannot entirely avoid. This trend seems to mirror the growing importance of former law enforcement officials in banks. In its inversion of former relations of dependence (previously it was the banks that recruited police personnel), it illustrates the routinization of the relations between two separate professional universes.

Information exchange is a crucial resource for *anticipating* risks, as it allows different actors to join forces in order to stop certain types of offenders. This form of cooperation has played a key role in the development of 'intelligence-led policing' in the field of law enforcement (Ratcliffe, 2008). From the police's point of view, the objective of such cooperation is not only to *anticipate* threats and risks, but also to *influence* decisionmaking (Ratcliffe, forthcoming). From the point of view of the banks, information obtained from law enforcement agencies complements the alerts provided by software tools in relation to decisionmaking. The implementation of AML/CTF computer technologies has been a strong driver for the development of information swaps.

Conclusion

In this article, we have shown that the involvement of French banks in AML/CTF tasks has grown considerably since the 'war on terror' was first launched in 2001. This is particularly true for the huge retail banks, because corporate and investment banks, along with private banking, are less concerned with large customer-screening tasks. Within the banks, AML/CTF programmes have relied on a risk-based management approach and have encompassed a wide range of measures. This new involvement has entailed the creation of decisionmaking processes to assist in dealing with doubts, suspicions, reporting and acceptable risk levels. Software tools and databases have also been purchased in order to support decisions in this field. In France, as elsewhere, use of these tools has been based on the need to secure the reputation and auditability of banks (Ericson, 2006). Their use has also fuelled logics of exclusion, owing to the ways in which software tools were set up to target (particular) individuals or social groups.

AML/CTF management, however, has not been limited to institutional change within the banks, as banks have also needed to take part in new and sometimes unexpected professional networks. First, compliance officers at both the national and the regional level have begun to exchange information with their counterparts in other banks. Second, they have begun to cooperate with law enforcement agencies on an everyday basis, more or less formally, through the creation of new professional ties that few would have anticipated two decades ago. Many banks have hired specialists from ranks of the judicial and law enforcement professions in order to benefit from their knowledge and professional ties. However, even in banks that have not opted for such a recruitment policy, compliance officers have sought to build new working routines with law enforcement and intelligence agents. Their interactions with Tracfin are based on formal and informal modes of communication. They also take part in informal meetings with police officers and exchange information with them.

The term 'public–private partnership' seems somewhat inappropriate for defining relationships between banks and law enforcement agencies, as 'complex new interplays of public and private' (Amoore and De Goede, 2008a: 13), relying on expertise, knowledge and databases, are now observable in the field. It should be borne in mind that banks have been forced to comply with AML/CTF policy, and that the 'partnership' was clearly imposed 'by command' (Ayling and Grabosky, 2006) – that is, by the government. Of the 76 people we interviewed, it was only Tracfin officials that used the term 'partnership'. The relationships between banks and law enforcement that have been established and that have now become commonplace reflect a new interdependence. Governmental agencies need the banks in order to access information on bank customers whose activities they may already be monitoring (Ericson and Haggerty, 1997; Williams, 2005a), while banks seek information on 'suspicious' customers in order to confirm or counter any doubts they might have.

Our main finding about the routinization of professional relationships between banks and the police invites us to reconsider the AML/CTF drive as a form of governmentality. Banks were certainly forced to comply with sovereign governmental requirements, but they are nevertheless responsible for the ways in which AML/CTF policy is organized and conducted in their agencies. Everyday banking practices show that governmentality in this field is not the result of an univocal intentionality. In the fight against 'dirty money', some players are seeking to combat terrorism (the police and some compliance officers), while others are seeking to preserve the international financial system (the International Monetary Fund, the Basel Committee). Within the banks, compliance officers seek to protect their firms against regulatory sanctions and, by so doing, they act as 'petty sovereigns' to exclude some types of customers from the international financial system. This assemblage of motivations and logics leads to the development of professional cooperation and the building of the new complex interplays we have described.

The main result of two decades of the fight against 'dirty money' is that banks have now been integrated into intelligence-led policing missions. They contribute to anticipating future risks and influencing decisionmakers (Ratcliffe, 2008: 89). They co-produce financial intelligence with law enforcement agencies, a practice that reflects the blurred borders of contemporary surveillance (Haggerty and Ericson, 2006). This finding is important, as such a 'security assemblage' (Abrahamsen and Williams, 2009) fits every shift in the definition of what 'dirty money' is. At the global level, dirty money has always been a moving target whose definition depends on international priorities from drug offences to organized crime and terrorism financing. Since the mid-2000s, the fight against this 'chameleon threat' (Mitsilegas, 2003) has focused more and more on the financing of nuclear proliferation. The co-production of intelligence by law enforcement

agencies and banking establishments is ready to work for each of these cases, as well as for other potential 'public bads' and future global threats. Professional routines are likely to last longer than the changing priorities of the fight against 'dirty money'.[7]

Acknowledgements

This article was translated by John Atherton and Uri Ben Gal. We would like to thank Anthony Amicelle, Charlotte Esptein, Nadège Ragaru and *Security Dialogue*'s anonymous reviewers for their helpful comments.

Notes

1. The Banking Commission (*Commission Bancaire*) acts as watchdog over the French banking and financial system, ensuring that credit institutions comply with the legal and regulatory provisions in force. It has the power to impose administrative penalties or financial sanctions on offenders.
2. Foucault (1990: 97) wrote that if Machiavelli provoked a scandal by thinking about 'the power of the Prince in terms of force relationships, perhaps we need to go one step further, do without the persona of the Prince, and decipher power mechanisms on the basis of a strategy that is immanent in force relationships'.
3. FATF is an intergovernmental body that sets standards in this field. For further details, see www.fatf-gafi.org.
4. According to one Tracfin interviewee, this amount does not concern cases of terrorism financing.
5. As for banks, they keep a copy of each report, which is entered into the network's common database. Following a search, this report can thus end up in the legal case file or even in the press. Owing to the vagueness of regulatory guidelines, banks generally keep SARs on file for ten years.
6. Former name of the defence ministry intelligence service (now known as the Direction générale de la sécurité extérieure [DGSE])
7. This finding might be compared with Simon's (2007: 263) conclusions that show that the main result of the war on drugs was the creation of new federal–local networks – that is, the establishment of professional relationships between agencies that previously were not involved in cooperative activities.

References

Abrahamsen R and Williams MC (2009) Security beyond the state: Global security assemblages in international politics. *International Political Sociology* 3(1): 1–17.

Amoore L and De Goede M (2008a) Governing by risk in the war on terror. In: Amoore L and De Goede M (eds) *Risk and the War on Terror*. New York: Routledge, 5–21.

Amoore L and De Goede M (eds) (2008b) *Risk and the War on Terror*. New York: Routledge.

Aradau C and Van Munster R (2008a) Governing terrorism through risk: Taking precautions, (un)knowing the future. *European Journal of International Relations* 13(1): 89–115.

Aradau C and Van Munster R (2008b) Taming the future: The dispositif of risk in the war on terror. In: Amoore L and De Goede M (eds) *Risk and the War on Terror*. New York: Routledge, 23–41.

Aradau C and Van Munster R (2009) Exceptionalism and the 'war on terror'. *British Journal of Criminology* 49(3): 686–701.

Ayling J and Grabosky P (2006) Policing by command: Enhancing law enforcement capacity through coercion. *Law and Policy* 28(4): 417–440.

Beck U (2002) The terrorist threat: World risk society revisited. *Theory, Culture & Society* 19(4): 39–55.

Biersteker T and Eckert S (eds) (2007) *Countering the Financing of Terrorism*. New York: Routledge.

Bush GW (2002) Speech at West Point, 1 June. Available at:http://georgewbush-whitehouse.archives.gov/news/releases/2002/06/20020601-3.html' (accessed 3 January 2011).

Butler J (2004) *Precarious Life: The Powers of Mourning and Violence*. London: Verso.

Callon M (1986) Some elements of a sociology of translation: Domestication of the scallops and the fishermen of St Brieuc Bay. In: Law J (ed.) *Power, Action and Belief: A New Sociology of Knowledge*. London: Routledge & Kegan Paul, 196–233.

Callon M, Lascoumes P and Barthe Y (2009) Measured action or how to decide without making a definitive decision. In: Callon M, Lascoumes L and Barthe Y (eds) *Acting in An Uncertain World: An Essay on Technical Democracy*. Cambridge, MA: The MIT Press, 190–223.

Canhoto AI (2007) *Profiling Behaviour: The Social Construction of Categories in the Detection of Financial Crime*. London: Department of Management., London School of Economics and Political Science.

c.a.s.e. collective (2006) Critical approaches to security in Europe: A networked manifesto. *Security Dialogue* 37(4): 443–487.

De Goede M (2007a) Financial regulation in the war on terror. In: Assassi L, Wigan D and Nesvetailova A (eds) *Global Finance in the New Century: Beyond Deregulation*. London: Palgrave, 193–207.

De Goede M (2007b) Underground money. *Cultural Critique* 65(Winter): 140–163.

Dean M (1999) *Governmentality: Power and Rule in Modern Society*. London: Sage.

Dupont B (2011) Governing security. In: Kramar K (ed.) *Criminology: Critical Canadian Perspectives*. Toronto: Pearson, 205–222.

Edwards J and Wolfe S (2006) A compliance competence partnership approach model. *Journal of Financial Regulation and Compliance* 14(2): 140–150.

Epstein C (2007) Guilty bodies, productive bodies, destructive bodies: Crossing the biometric borders. *International Political Sociology* 1(2): 149–164.

Ericson R (2006) Ten uncertainties of risk-management approaches to security. *Revue canadienne de criminologie et de justice pénale* 48(3): 345–359.

Ericson R and Haggerty K (1997) *Policing the Risk Society*. Toronto: University of Toronto 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): 1–20.

Favarel-Garrigues G, Godefroy T and Lascoumes P (2009) *Les sentinelles de l'argent sale au quotidien. Les banques aux prises avec l'antiblanchiment* [Dirty Money Sentinels: Banks and Anti-Money Laundering]. Paris: La Découverte.

Financial Action Task Force/Groupe d'Action Financière (FATF-GAFI) (2007) *Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures*. Paris: FATF-GAFI.

Foucault M (1976) *Histoire de la sexualité, vol. 1: La volonté de savoir* [The History of Sexuality Vol. 1: The Will to Knowledge]. Paris: Gallimard.

Foucault M (1990) *The History of Sexuality, Vol. 1: An Introduction*. Trans. Robert Hurley. New York: Vintage.

Foucault M ([1978] 1994) La gouvernementalité [Governmentality]. In: *Dits et écrits Tome III* [Interviews and writings, Vol. III]. Paris: Gallimard.

Freestone D and Hey E (1996) *The Precautionary Principle and International Law*. The Hague: Kluwer Law International.

Gallati R (2003) *Risk Management and Capital Adequacy*. New York: McGraw-Hill.

Gandy O, Jr (2006) Data mining, surveillance, and discrimination in the post-9/11 environment. In: Haggerty K and Ericson R (eds) *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press, 363–385.

Gelemerova L (2009) On the frontline against money-laundering: The regulatory minefield. *Crime, Law and Social Change* 52(1): 33–55.

Gilligan G (2009) PEEPing at PEPs. *Journal of Financial Crime* 16(2): 137–143.

Haggerty K and Ericson R (eds) (2006) *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press.

Hardouin P (2009) Banks governance and public–private partnership in preventing and confronting organized crime, corruption and terrorism financing. *Journal of Financial Crime* 16(3): 199–209.

Harvey J (2004) Compliance and reporting issues arising for financial institutions from money laundering regulations: A preliminary cost benefit study. *Journal of Money Laundering Control* 7(4): 333–346.

Harvey J (2008) Just how effective is money laundering legislation? *The Security Journal* 21(3): 189–211.

Harvey J and Fung Lau S (2009) Crime-money, reputation and reporting. *Crime, Law & Social Change* 52(1): 57–72.

Helleiner E (1999) State power and the regulation of illicit activity in global finance. In: Friman HR and Andreas P (eds) *Illicit Global Economy and State Power*. Boulder, CO: Rowman and Littlefield, 53–90.

Heng YK and McDonagh K (2009) *Risk, Global Governance and Security: The Other War on Terror*. New York: Routledge.

Holzer B and Millo Y (2005) From risks to second-order dangers in financial markets: Unintended consequences of risk management systems. *New Political Economy* 10(2): 223–246.

Hornqvist M (2010) *Risk, Power and the State After Foucault*. Stockholm: Routledge-Cavendish.

Jobst A (2007) It's all in the data: Consistent operational risk measurement and regulation. *Journal of Financial Regulation and Compliance* 15(4): 423–449.

Langley P (2009) *The Everyday Life of Global Finance: Saving and Borrowing in Anglo-America*. Oxford: Oxford University Press.

Levi M (1991) *Pecunia non olet*: Cleansing the money-launders from the temple. *Crime, Law & Social Change* 16(3): 217–302 .

Levi M (2003) Organised and financial crime. In: Newburn T (ed.) *Handbook of Policing*. Cullompton: Willan, 444–467.

Levi M (2007) *Pecunia non olet?* The control of money-laundering revisited: Cleansing the money-launderers from the temple. In: Bovenkerk F and Levi M (eds) *The Organized Crime Community: Essays in Honor of Alan A. Block*. Dordrecht: Springer, 161–182.

Levi M and Wall D (2004) Technologies, security, and privacy in post 9/11 European information society. *Journal of Law and Society* 31(2): 194–220.

Lyon D (2003) Surveillance after September 11. In: Ball K and Webster F (eds) *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Era*. London: Pluto, 16–25.

Lyon D (2006) 9/11, synopticon, and scopophilia: Watching and being watched. In: Haggerty K and Ericson R (eds) *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press, 35–55.

McCue C (2006) *Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis*. Oxford: Butterworth-Heinemann.

Martin R (2007) *An Empire of Indifference: American War and the Financial Logic of Risk Management*. Durham, NC: Duke University Press.

Mitsilegas V (2003) Countering the chameleon threat of dirty money: 'Hard' and 'soft' law in the emergence of a global regime against money laundering and terrorist finance. In: Edwards A and Gill P (eds) *Transnational Organized Crime: Perspectives on Global Security*. London: Routledge, 195–211.

Mizruchi M and Stearns L (2001) Getting deals done: The use of social networks in bank decision-making. *American Sociological Review* 66(5): 647–71.

Mythen G and Walklate S (2006) Criminology and terrorism: Which thesis? Risk society or governmentality? *British Journal of Criminology* 46(3): 379–398.

Naylor T (1997) *The Big Wash: An Enquiry into the History and Practice of Money-Laundering*. Montreal: McGill University.

Naylor T (2006) *Satanic Purses: Money, Myth, and Misinformation in the War on Terror*. Montreal: McGill Queen's University Press.

O'Riordan T and Cameron J (1994) *Interpreting the Precautionary Principle*. London: Earthscan.

Power M (2003) The invention of operational risk. Discussion paper no.16. London: Centre for Analysis of Risk and Regulation, London School of Economics and Political Science.

Power M (2004) *The Risk Management of Everything*. London: Demos.

Power M (2007) *Organizing Uncertainty: Designing a World of Risk Management*. Oxford: Oxford University Press.

Pradier PC (2006) *La notion de risque en économie* [The Concept of Risk in Economics]. Paris: La Découverte.

Rasmussen MV (2006) *The Risk Society at War: Terror, Technology and Strategy in the Twenty-First Century*. Cambridge: Cambridge University Press.

Ratcliffe J (2008) *Intelligence-Led Policing*. Cullompton: Willan.

Ratcliffe J (2010) Intelligence-led policing: Anticipating risk and influencing action. In: Peterson MB, Morehouse B and Wright R (eds) *Intelligence 2010: Revising the Basic Elements*. Richmond: IALEIA.

Sheptycki J (2000) Policing the virtual launderette: Money laundering and global governance. In: Scheptycki J (ed.) *Issues in Transnational Policing*. London: Routledge, 134–176.

Simon J (2007) *Governing Through Crime: How the War on Crime Transformed American Democracy and Created a Culture of Fear*. Oxford: Oxford University Press.

Stenning P (2009) Governance and accountability in a plural policing environment: The story so far. *Policing* 3(1): 22–33.

Van Duyne P (1998) Money-laundering: Pavlov's dog and beyond. *The Howard Journal* 37(4): 359–374.

Verhage A (2009) Between the hammer and the anvil? The anti-money laundering-complex and its interactions with the compliance industry. *Crime, Law and Social Change* 52(1): 9–32.

Vlcek W (2008) A leviathan rejuvenated: Surveillance, money laundering, and the war on terror. *International Journal of Politics, Culture, and Society* 20(1–4): 21–40.

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

Williams J (2005b) Governability matters: The private policing of economic crime and the challenge of democratic governance. *Policing & Society* 15(2): 187–211.

Wood J and Dupont B (eds) (2006) *Democracy, Society and the Governance of Security*. Cambridge: Cambridge University Press.

Yeandle M, Mainelli M, Berendt A and Healy B (2005) *Anti-Money Laundering Requirements: Costs, Benefits and Perceptions*. London: Corporation of London. Available at: http://www.icaew.com/index.cfm/route/144554/icaew_ga/pdf (accessed 20 December 2010).

Zedner L (2006) Liquid security: Managing the market for crime control. *Criminology & Criminal Justice* 6(3): 267–288.

Gilles Favarel-Garrigues is a CNRS Research Fellow at Sciences Po/CERI, Paris. He recently co-edited (with Jean-Louis Briquet) *Organized Crime and States: The Hidden Face of Politics* (Palgrave Macmillan, 2010). His book *Policing Economic Crime in Russia: From Planned Economy to Privatization* will be published by Hurst (London) and Columbia University Press (New York) in 2011.

Thierry Godefroy is a CNRS Research Fellow at CESDIP, Guyancourt. He has recently published with (Gilles Favarel-Garrigues and Pierre Lascoumes) *Les sentinelles de l'argent sale. Les banques aux prises avec l'antiblanchiment* [Dirty Money Sentinels: Banks and Anti-Money Laundering] (La découverte, 2009).

Pierre Lascoumes is CNRS Research Director at Sciences Po/CEE, Paris. He has recently published (with Michel Callon and Yannick Barthe) *Acting in an Uncertain World: An Essay on Technical Democracy* (MIT Press, 2009) and *Favoritisme et corruption à la française, petits arrangements avec la probité* [Favouritism and Corruption French-Style: Playing with Probity] (Presses de Sciences-Po, 2010).