Public-Private Partnerships in the Fight against Terrorism

Abstract: Based on a case study of the role of private financial institutions in the fight against terrorist financing, this article examines the rationales for, and actual results of, public-private partnerships in counterterrorism. It shows that there is still a lack of appreciation of the roles that regular private business play, both willingly and unwillingly, in the fight against terrorism. As profit, rather than security, maximizers, private sector actors may decide to take certain security risks rather than addressing them directly, which is in contrast expected from public agencies. As a consequence, public-private partnerships have not been the silver bullet that the representatives of public agencies had hoped for since 9/11. In fact, to many private sector representatives, they are more akin to public-private dictatorships.

Keywords: Public-private partnerships, private actors, terrorism, counterterrorism, terrorist financing, security.

Introduction

Terrorism is often cited as a key threat to (inter-)national security and as such, the fight against it is generally considered to be a key task for governments worldwide. In several areas of the post-9/11 fight against terrorism, however, private rather than public entities have shouldered the bulk of the burden. This has recently been recognized in several national security strategies as well as in the academic literature, which in particular refer to public-private partnerships (PPPs) as a key component in the fight against contemporary terrorism. Nevertheless, there is still a substantial lack of appreciation of the many roles that various private actors play, both willingly and unwillingly, in the fight against terrorism. Based on a case study of the role private financial institutions in the fight against terrorist finances, I argue that the currently prevailing public authorities’ vision of PPPs as security enhancers is fundamentally misconceived because regular private businesses are still primarily concerned about making profit.

The structure of the article is as follows. In the first section provides an overview of rationales for the inclusion of private sector actors and the establishment of public-private partnerships in the fight against terrorism. The
Role of Private Actors and Public-Private Partnerships in the Fight against Terrorism

The increasing role of private actors in both national and international security has been discussed at least since the end of the cold war. [37, 66] In the last decade, the primary focus of these debates concerned the intriguing questions arising from the increasing utilization of services of Private Military and/or Security Companies (PMSCs). [3, 13, 33, 47, 49, 55] Pointing out to the massive use of PMSCs in the US-led war on terror, some authors have even argued that “[t]he private sector is so firmly embedded in combat, occupation and peacekeeping duties that the phenomenon may have reached the point of no return: the US military would struggle to wage war without it.” [60] The bulk of this literature offers a critical view of those private actors that do security for profit (PMSCs), but it does not shed much light on counterterrorism beyond the US-led wars in Iraq and Afghanistan. Moreover, it is not dealing with the role of regular private sector actors, who in general do not sell security-related products and/or services. Since 9/11, however, many regular private businesses have actually shouldered the bulk of the burden in several areas of counterterrorism. In particular, this has been the case in the protection of critical infrastructure, which is considered as a likely target of future terrorist attacks. While there is still some debate about what makes a particular infrastructure critical to the extent that its
incapacity or destruction would have a debilitating effect on national security,¹ there is a consensus that much of it is owned and/or operated by the private sector. According to the 9/11 Commission Report, for example, the private sector controls 85 percent of the critical infrastructure in the US, so “unless a terrorist's target is a military or other secure government facility, the "first" first responders will almost certainly be civilians.” [59] Due to privatization and deregulation of the public sector since the 1980s and the globalization processes since the end of the cold war, a similar state of affairs can be found in most Western countries.

The role of private sectors actors has, nevertheless, not received much attention in the terrorism and counterterrorism literature thus far. Among the few notable exceptions, Gelemerova has argued that although promulgated by public bodies, the achievement of many objectives of counterterrorism efforts requires various “market players to become watchmen and report suspicious or unusual activities to ‘the competent [public] authorities.’” [27] Referring to the large number of both public and private actors involved in various counterterrorism efforts, where “[p]revention, detection and reporting are carried out by private partners, while the public partners have an analytic and repressive task,” [64] several authors went a step further and suggested that we are witnessing the emergence of new types of security arrangements. Building on Foucault’s notion of space,² Wesseling has described the European fight against terrorism financing as “a network of all private and public, national and international actors that are responsible for standard setting, decision-making, implementing and/or monitoring the EU’s measures to combat terrorism finance.” [67] Alternatively, building on Foucault’s conception of power,³ Favarel-Garrigues et al. have argued that many of the current counterterrorism efforts represent a form of neoliberal 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 originality of these apparatuses lies in their

---

¹ The most frequently listed examples include banking and finance, government services, telecommunications and information and communication technologies, emergency and rescue services, energy and electricity, health services, transportation, logistics and distribution and water supply. [18]
² According to Foucault, the notion of ‘space’ does not imply a fixed geographical area it is rather a constructed transnational “network that connects points and intersects with its own skein.” [25]
³ 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). [24]
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. [21]

Finally, Parker and Taylor suggested that we are witnessing the emergence of “a new security paradigm in which financial borders and parameters are best understood as a ‘complex assemblage’ in which private financial institutions are in effect, authorized to make security decisions.” [48]

In all of the aforementioned conceptualizations of the role of private actors in the fight against terrorism, one can detect the blurring of public and private authority and an increasingly important role of the latter when it comes to the day-to-day efforts to tackle terrorist activities. This corresponds to the more general conclusions of the security governance scholarship, which has pointed out that in response to the emergence of new security threats in the last decade, there has been a turn towards new modes of security governance that include a hybrid mix of public and private actors, rest upon non-hierarchical networks, and rely on soft compliance based on instruments such as peer evaluations or best practices. [28,36,37,66] Because of their flexibility, relative independence from national governments, as well as their ability to include a broad range of participants on equal footing, it is generally assumed that these informal policy structures “are more suitable for tackling governance problems or achieving common goals than more hierarchical and formal strategies.” [16] Importantly for this article, this conclusion should also be applicable to the fight against the worldwide network of Al-Qaeda cells – the claim being that the best way to counter terrorist networks is to create counterterrorism networks. [29]

Overall, it can therefore be argued that notwithstanding the critical voices concerning the use of PMSCs’ services, the available literature presents the role of private actors in the fight against terrorism as a necessity. Moreover, although there are many different ways for involving private actors in the provision of security, public-private partnerships have become particularly popular option in the context of counterterrorism in the last decade. Originally conceived in the field of administrative reform and the concept of New Public Management in 1980s with the dual aim of debureaucratization of public services and privatization promotion, [47] the concept of public-private partnerships has been
subsequently also utilized within the then new concept of critical infrastructure protection in the 1990s as a way to reduce vulnerability of vital systems to low-probability, yet high-consequence new security threats, including terrorism. [14] Since 9/11, the popularity of public-private partnerships in the context of terrorism rose further to the point that they were described by some public officials “as the third leg in an approach to terrorism – the first two being intelligence and surveillance (or technology).” [50] The representatives of US security agencies, for example, argued that the fight against terrorism “is the responsibility of more than law enforcement and government – it is a shared mission of all people. Partnerships between the public and private sector represent one of the strongest means to detect, deter, disrupt and deny terrorist and other criminal organizations illicit profits and material support required to fuel their evil acts.” [23] Moreover, it was also suggested the private sector has much to gain from cooperating with the public security agencies:

[B]ecause they can coordinate their plans in advance regarding evacuation, transportation, and other issues; gain intelligence from law enforcement regarding threats and crime trends, develop relationships so that they will know who to contact for help or to report information; build law enforcement’s understanding of corporate needs, such as confidentiality; and boost law enforcement’s respect for the security field. [15]

As such, at least by the representatives of public security agencies, public-private partnerships in the fight against terrorism have often been presented as win-win solutions to both the public and private sector actors.

In the following sections of this article, the optimism of public officials regarding the role of PPPs in counterterrorism is subjected to scrutiny in a case study of one crucial area of the post-9/11 counterterrorism efforts – the fight against terrorist financing, where there is little doubt that the first line responders are not agents of public authorities but employees of private financial institutions. Although additional case studies of other areas of counterterrorism would be needed to verify the relevance of its findings beyond the fight against terrorist financing, it is possible to argue within the limited space of one article that PPPs have not been the silver bullet that the representatives of public agencies had hoped for since 9/11. This is problematic because many have hoped that measures to fight terrorist financing (FTF) should also mitigate the first mover advantage

---

4 The usual list of new security threats includes terrorism, organized crime, and proliferation of
terrorist otherwise hold. [6] In addition, FTF efforts should also help to track operatives, chart relationships, and deter individuals from supporting terrorist organizations both directly [17] and indirectly, through diversion of funds from charitable and other organizations. [6] Moreover, unlike much of the other evidence relating to terrorism, which can be “suspect, the product of interrogation, rewards, betrayals, decepts … a financial record doesn’t lie.” [63] As such, it is supposed to be more reliable than other forms of intelligence when it comes to reconstructing events after terrorist attacks and gaining better understanding of the terrorist group’s modus operandi and internal organization.

Case Study of Public-Private Partnerships in the Fight against Terrorist Financing

The fight against terrorist financing is predicated upon a straightforward logic – terrorists, like everyone else in modern societies, need money to survive and function. If the money can be shut down, so can the terrorist activities that it was meant to finance. Shutting down terrorist finances, however, has proven to be a formidable task due to 1.) the global nature of contemporary terrorism that in turn necessitates uniform international implementation of FTF measures; and 2.) the seemingly never-ending dispute about the definition of terrorism, [54] which complicates both academic research and practical counterterrorism efforts at the international level. Moreover, terrorist groups vary in their organizational form and thus also in the ways they raise, store and move funds. [6] Prior to 9/11, terrorism was financed on national basis through criminal activities (protection rackets, bank robberies etc.); and/or on transnational basis through fundraising in states with sizeable diasporas for the armed struggle in the “home” state; and/or through states funding foreign groups as proxies for the achievement of their own foreign policy goals. After 9/11, however:

[T]he advent of self-supporting ‘nomadic terrorist networks’ with global or regional, rather than separatist, goals, such as al-Qaeda, has added a new dimension to the problem. A nomadic group moves between jurisdictions and operates in different jurisdictions. It can obtain its financing in one region, but carry out operations by means of active cells stationed in, or transferred to, another region. [12]
Thus, in order to “starve the terrorists of funding, turn them against each other, rout them out of their safe hiding places, and bring them to justice,” [10] several parallel national, regional and global FTF processes have been put in place since the 1970s.

As discussed elsewhere, these processes interact and overlap in numerous ways but it is possible to identify two key contemporary FTF frameworks whose logic has, at least since 9/11, shaped FTF efforts worldwide – the smart sanctions model advanced by the United Nations (UN) Security Council and the anti-money laundering model advanced by G-7’s Financial Action Task Force (FATF). [9, 61, 65] Generally speaking, UN smart sanctions work by creating a Sanctions Committee which draws up a “blacklist” of targeted persons and/or groups and obliges all UN Member States to freeze the listed persons’ assets, impose travel bans on them and criminalize any attempts to provide them with financing or weapons. The FATF model is based on the Forty Recommendations for pursuing the fight against money laundering and Nine Special Recommendations (9SR)\(^5\) focused more specifically on terrorist financing, which nonetheless also assume the existence of major similarities of anti-money laundering and FTF processes. Although there is no binding obligation to enforce either of them,\(^6\) they are nowadays widely recognized as the international standard in the fight against terrorist finances. Most importantly for the purposes of this analysis, the day-to-day execution of both the UN-led smart sanctions and the FATF anti-money laundering models depends on the work of private financial institutions (such as banks, insurance and investment companies), as well as certain non-financial organizations (such as lawyers, guarding companies or casinos and dealers in high-value goods). They are supposed to contribute to the public FTF efforts by adopting “a risk management process for dealing with money laundering and terrorism financing” which 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.” [22] More specifically:

Banks are expected to establish and maintain effective [customer due diligence] CDD measures at the point of establishing a customer relationship and on an on-going basis as necessary thereafter, the

\(^5\) The list of 9 Special Recommendations is available at: http://www.fatf-gafi.org/document/9/0.3343_en_32250379_32236920_34032073_1_1_1_1.00.html.

\(^6\) The UN Security Council has stopped short of adopting a Chapter VII resolution ordering states to enforce the FATF’s recommendations, but it has “strongly urged” them to do so in resolution no. 1617.
maintenance of adequate records, the ability to identify suspicious transactions and file STRs as necessary, the use of comprehensive programs for the training of staff, and the maintenance of effective compliance and internal audit mechanism. [35]

These measures should allow private financial institutions to detect suspicious transactions and/or customers, which in turn they are obliged to report for further analysis to designated public bodies – the financial intelligence units (FIUs).

Known as Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs), they differ in their scope and their legal definition as well as method of collection is specified by each state. In general, however, they usually contain the following fields: the reasons for suspicion, information on the transaction (such as the place, date, time or period of time in which the suspicious acts occurred), the currency and the amount of money involved, extensive personal identification details, the official address of the customer, and account/credit card numbers of the persons or companies involved, the financial instruments (cash, checks, credit cards, e-money etc.), number of transactions, status of the transactions, detailed information on the objects involved and the countries and institutions concerned by the transaction, information on the institution making the declaration, and a field to further describe the situation in more detail. The FIUs’ personnel review the reported SARs in order to discover terrorist financing by searching through their databases “for certain characteristics such as combinations of specific countries, names and amounts of money. These searches can be combined with information from a range of other sources such as law enforcement, administrative or public registers, information and databases from private companies and open sources, most importantly the Internet search tool Google.” [67] The precise procedure, database access, and follow-up on positive SARs varies from country to country, depending on the type of the national FIU.7

The more important point is that while the entire process appears to be clear in theory, it has been far more challenging to ensure proper utilization of the aforementioned FTF measures in practice. In particular, the expected public-private partnerships in the fight against terrorist finances have been largely rendered meaningless due to the fact that private financial institutions have

7 Among the EU Member States, for example, 12 FIUs are administrative FIUs, 11 FIUs have a law enforcement basis, 3 FIUs are hybrid or independent and one is judicial.
massively resorted to the practice of defensive SAR filings that report even marginally irregular activity. Also referred to as the practice of “umbrella reports,” [21] it has become the primary mechanism of financial institutions’ compliance officials who are coping with many FTF requirements by “doing enough to proverbially ‘cover their backs.’” [30] Even though officials in some FIs’ have vehemently denied following a simple “cover your ass” policy in anonymous interviews, [64] the available data on the amount of SARs points to the contrary. Although much information in many countries is still secret and the differences in national definitions of a suspicious activity/transaction obscure cross-country comparisons, table 1 clearly indicates that the overall number of SARs submitted to national FIUs has increased over the years since 1994, with major hikes following the 9/11 terrorist attacks and the subsequent introduction of the smart-sanctions and anti-money laundering models to fight terrorist financing.

[Table 1 somewhere here]

The problem with the “cover your ass” policy is that the “efficiency” of private FIs in meeting the public FTF requirements by filling a high number of SARs does not necessarily translate into effectiveness in the fight against terrorist financing. In addition to placing a substantial burden on the public FIUs which have to process a large amount of data of dubious value, the increasing number of reported transactions serves to further bury suspicious transactions actually indicative of terrorist financing, which represent only a small share of the reported SARs. Thus, some experts, such as the president of the British Association of Certified Fraud Examiners, believe that “the system can actually help criminals” because “firms are now disclosing so much because of the fear of prosecution that there is a danger of serious infringements being hidden by and lost under all the noise of all the minor problems and unfounded suspicions.”8 This was also confirmed in a study by the International Monetary Fund, which found the “cover your ass” policy as strikingly similar to the effects of the so-called Theory of “Crying Wolf:”

[E]xcessive reporting … fails to identify what is truly important by diluting the information value of reports. The intuition can be best understood through an analogy with the tale: “The boy who cried wolf”. In

8 Cited in [65]
the tale, the boy cried wolf so often, that his cries became meaningless. Similarly, excessive reporting, which will be referred to as “crying wolf”, fails to identify what is truly relevant. [56]

Moreover, the study also revealed that the relation between the height of the sanctions imposed on FIs for non-compliance and the effectiveness of the whole AML process until conviction can be depicted in a Laffer curve: if sanctions get too high their impact on effectiveness is negative.

Although the criteria for measuring effectiveness of FTF policies are still up to debate due to the difficulties of establishing causality between output, outcome, and impact, [7] the available data confirms that high reporting efficiency by FIs has thus far not led either to depriving the terrorist of more funding or in locking them up behind the bars in large numbers. Regarding the former, the available data shows that higher numbers of SARs have not led to higher amounts of frozen terrorist assets (see figure 1). Regarding the latter, only the experiences of few FATF jurisdictions indicate some “usefulness” of the money laundering model at the operational level. In most other countries, however, the pattern is often reversed and evidence of money laundering/terrorist financing comes to light during the course of other criminal investigations. According to a Eurostat study, for example, out of 17 EU Member States that provided data on the number of cases initiated by law enforcement agencies on the basis of Suspicious Transaction Reports sent by the national FIUs in 2007 and 2008, ten countries reported less than 100 cases annually. [9] Given the low number of terrorist related reports, one can therefore concur with Cameron that “there is little cause to believe that the mechanisms put in place will allow more than sporadic detection of terrorist financing. To the extent, then, that these measures have been ‘sold’ as means of preventing terrorist outrages this certainly represents a misrepresentation.” [12] Indeed, there have been only few convictions thus far for violations of FTF laws. In the UK for example, there have been about 10 convictions for FTF offences out of a total of about 100 convictions under the entire spectrum of the existing counterterrorism legislation. [7]

[Figure 1 somewhere here]

9 The remaining EU Member States reported between 132-906 cases for 2008. Only in the case of Germany, where all STRs are legally bound to result in the initiation of criminal proceedings, the number exceeded 1000 cases (7,349 in 2008). [57]
Pessimism about the effectiveness of existing FTF measures is also apparent from the few available national case studies and surveys of FIs’ employees. According to a case study on the role of French banks in FTF, for example, 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.’” [21] Similarly, an evaluation of the Dutch FTF system showed that high numbers of reports do not automatically result in a higher effectiveness of the system. Furthermore, it suggested that “introducing measures just to increase the number of reports, may only result in a widening of the gap between public and private actors within the AML complex, as the usefulness of the system is increasingly questioned by the private institutions.” [64] In a 2004-2005 survey of the UK financial services industry, almost two-thirds of the respondents said the existing AML measures were too severe in proportion to the risks of money laundering. They „clearly believe that the UK has approached a ‘tipping point’ where past, current and future costs of such legislation are perceived to be greater than the benefits.” The survey also revealed that “[o]verall, UK-based companies comply with AMLR in order to avoid sanctions from the authorities, and not because they perceive AMLR as representing good business practice or as being effective at combating money laundering.” [68] Another survey among banks in Switzerland, Germany and Singapore found that “the AML rules’ implementation is highly burdensome and causes significant costs and efforts throughout the banks” and that “the impact of money laundering prevention on the predicate offences is small.” [26] Finally, 77 percent of the interviewed Belgium compliance officers also complained that the government saddles the banking sector with governmental tasks: “This gives rise to the interpretation that the AML complex is mainly a one-way street in which private actors need to invest, while receiving very little in return.” [64]

**Why are Public-Private Partnerships in the Fight against Terrorist Financing far from a Silver Bullet?**

The findings of the case study of the role of private financial institutions in the fight against terrorist financing suggests that PPPs are not automatically producing win-win solutions either for the public or the private sector. In addition,
the case study also suggests that perhaps too many public officials erroneously perceive public-private partnerships as the best answer to many problems resulting from the negative consequences of liberalization, privatization and globalization of critical infrastructures – e.g. those very processes that PPPs had been supposed to promote in the 1980s when the very concept of PPPs emerged. In this perspective, the primary aim of the contemporary public-private partnerships in the context of counterterrorism is no longer to raise efficiency, but to enhance security. As discussed in the following paragraphs, this rather fundamental change of focus points to a number of explanations for the less than perfect performance of PPPs in counterterrorism. In particular, three areas of concern can be detected when it comes to cooperation between private and public sector actors in counterterrorism: 1.) disagreements about the definition, scope and methods of analysis of the threat of terrorism; 2.) information sharing complications; 3.) the dissonance between the logic of security of public agencies and the logic of profit of private companies.

**Unclear Definitions, Disputed Data and Shaky Methodology**

Specific terrorist attacks are inherently difficult to predict with some theory and prevent with some practical countermeasures. The key problems include not just the seemingly never-ending disputes about the definition of terrorism. There is also a remarkable lack of analyses of the impact of adopted counterterrorism measures at all levels. As one analyst remarked, “it remains largely matter of faith that anti-crime and anti-terror efforts have some impact beyond the immediate operational outcomes.” [40] Thus, despite the billions spent annually on counterterrorism, we still lack an adequate performance evaluation baseline to figure out what works and why. To some extent, this is due to the methodological difficulties of finding the right proxy indicators that would complement the readily available, yet inherently limited quantitative criteria (such as the number of suspicious transaction reports or amounts of frozen terrorist money) that do not shed much light on the actual effects of counterterrorism measures on specific cultures, groups and individuals – even the most efficient counterterrorism measures increasing the overall security may be problematic due to their impact on other important values such as liberty and justice. In short, public (as well as
academic) authorities have been unable to clearly define the problem(s) and specify what exactly works in fixing them.

In case of the fight against terrorist financing, however, there is an additional set of difficulties that private FIs have had to address. The first concerns the applicability of the very logic of the risk assessment approach to FTF measures. Although risk management models are neither new nor uncommon to private sector actors, including FIs, they normally operate on the assumption that the company is able to quantify the extent of loss that would arise in the event that the risk occurs. For several reasons, however, this is extremely difficult, if not impossible, to do within the framework of the two aforementioned FTF models. Firstly, while there is data useful for developing risk assessment models for most types of business risk, the same cannot be said of the terrorist financing risks because it is rather difficult to assess how much money is actually being laundered. The International Monetary Fund (IMF) estimated the total as a figure equal to between 2% and 5% of the world’s GDP, e.g. up to $2 trillion annually. [5] However, the critics have challenged the credibility of the IMF’s methodology, claiming that “the only thing that can be stated with certainty is that the actual figure is not likely to be less than 0% or more than 100%.” [44] Such claims are further supported by the fact that even FATF’s attempts to calculate estimates of AML flows have failed in the past. [61] The data reported by the companies themselves in a 2007 survey by PriceWaterhouseCoopers suggests that although 12% perceived money laundering as a high risk to their organization, only 4% of these companies actually reported having experienced incidents related to money laundering. [51] One can therefore conclude with Verhage that “the perceived threat of money laundering … [is] higher than the actual occurrence.” [64] Most importantly, however, due to difficulties with establishing the proper magnitude of the terrorist financing risk, private FIs not only cannot estimate the significance of the money laundering problem but they are also left “with no clear benchmark of what would constitute success or of what an ‘acceptable’ figure for global laundered funds might be.” [61] As a consequence, it is not surprising that many FIs have concluded that it is better to err on the side of over-reporting anything that looks even remotely suspicious.
Secondly, although several international, national and private bodies have produced guidelines for identifying suspicious transactions, it is still not entirely clear how FIs are supposed to identify FTF risks:

[L]ittle or no specific guidance has been given as to how to determine whether or not a customer or a partner may be linked to or involved in terrorist financing. Is running the names of clients through databases of national and international blacklists and sanctions lists sufficient? Should banks and other reporting institutions watch out for connections to ‘countries of risk’? [27]

At the moment, it therefore appears that it up to the individual FIs to evaluate the transaction and customers on a largely discretionary basis: “Essentially, banks are now expected to make a value judgment about customers and their money and whether they may be involved in some terrorist activity, in the future.” [65] According to the aforementioned IMF report, the vagueness is actually intentional and should be understood as “another form of constructive ambiguity”:

The notion of suspicion is intentionally left vague so as to leave both money launderers and banks uncertain. Thus, money launderers cannot rely on simple rules to avoid being reported. Furthermore, banks are forced to constantly improve their understanding of how money laundering is done. [56]

In practice, however, the representatives of private FIs have criticized the fact that very few general clues for TF activities have been developed thus far: “A single financial transaction that raises suspicion could relate to anything. So the effectiveness of the reporting system depends heavily on the ingenuity of the analyst and on the other data he has available.” [34] Thus, although public officials hoped that the discretionary risk-based approach will help to increase the quality of SARs from the private sector, due to the absence of clear criteria, risk assessment in practice indeed appears to be largely based on the tenacity of AML/FTF compliance official/s in individual FIs. The problem is that although compliance departments vary in size, related to the size of the financial institution, ranging from one single compliance officer in smaller banks to seventy plus officers in large transnational FIs, [34] the magnitude of their task is daunting.

---


12 E.g. the Wolfsberg Group of Banks principles available at www.wolfsbergprinciples.com.
According to Cameron, just the New York InterBank system handles 200,000 payments totaling $1.1 trillion every day. [12]

(Lack of) Information Sharing between Public and Private Actors

It may be argued that one of the key purposes of establishing PPPs in counterterrorism is information exchange facilitation. [19] In practice, however, information exchange is far from being automatic. The relevant information is often extremely sensitive and available studies show that not only are governments often reluctant to share it with other governments, but the same applies to information sharing among national security agencies within many countries. [43] This reluctance is usually due to the absence of several prerequisites, most importantly a sense of mutual trust and a shared expectation of positive outcomes. Both of these take a very long time to develop and a “fundamental problem is that trust can only be developed through collaboration, which in turn also depends on trust.” [19] As among the public agencies, the dilemmas of information exchange between public and private actors are therefore a classic example of the chicken-and-egg paradox. [4, 8] To complicate things further, information sharing between public and private actors in the context of the fight against terrorist financing is compounded by four additional complications. Firstly, there are tens of thousands of various private financial institutions operating worldwide. Such numbers render trust-building extremely difficult, if not impossible if one adds the fact that private actors generally dislike admitting security vulnerabilities for the fear of being penalized by public regulatory bodies and/or exploited by private sector competitors. Furthermore, it is clear that in the context of the fight against terrorist financing one financial safe-heaven is enough to wrack any FTF efforts, whose strength and effectiveness are determined by the weakest link in the international cooperation frameworks.

Secondly, in the fight against terrorist financing, another challenge lies in the amounts of information that needs to be collected, filtered and exchanged. Given the vast number of transactions handled by private FIs on a daily basis, even the collection and filtering of information represents a daunting and costly challenge. It is therefore not surprising that even the biggest US banks with the best automated interdiction software acknowledge that some “leakage” is inevitable: “Large banking institutions handle millions of transactions each day
and, despite state of the art interdiction systems, frequent staff training and the institutions best efforts, it is statistically inevitable that a large bank will have inadvertent violations of sanctions.” [32] In the context of counterterrorism, this is again rather problematic given that according to the UN Analytical Support and Sanctions Monitoring Team “[o]nly the sophisticated attacks of 11 September 2001 required significant funding over six figures. Other Al-Qaeda terrorist operations have been far less expensive.” [62] The report specifically stated that the Madrid bombings in 2004 cost about $2,000 and the Report of the Official Account of the Bombings in London in July 2005 estimated that the London bombings cost less than £8,000. [31] Similarly, the available data on terrorist campaigns conducted by the “older” domestic terrorist groups in Europe indicates that they also do not require extensive funding to carry out deadly attacks.  

Thirdly, there are legal impediments to sharing classified information between public agencies and the private sector. In fact, the official UN terrorist list that all UN Member States are obliged to enforce, contains over 500 names of individuals and groups, 14 most of which were listed on the basis of secret intelligence material supplied by the MSs. As discussed extensively in the legal literature, this has generated a great deal of criticism and, in some countries, even court trials. [11, 45] In summary, it can be argued that despite some recent improvements, many of the existing mechanisms for listing and delisting of both individuals and groups considered to be terrorist still do not meet internationally recognized human rights standards, which include the right to judicial review, the right to procedural fairness, the right to be heard, and the right to judicial remedy. None of this encourages the private sector actors to share information with public authorities.

Fourthly, the current FTF blacklisting regime is neither smart nor targeted enough because the same sanction measures are applied against the direct and primary targets (such as Osama bin Laden in the past) and against a party who only incidentally dealt with or supported the primary target. Moreover, as The Economist pointed out, if Osama bin Laden “can recruit 30 people willing to die on his behalf, he will have no problem getting 100 to open bank accounts.” [58] It

13 Donohue estimated the annual costs of Provisional Irish Republican Army at £1.5 million but noted that some of the smaller IRA splinter groups, such as Continuity IRA, operated on a budget if £30,000 or less. [17]
14 For the most current list, see http://www.un.org/sc/committees/1267/consolist.shtml
is therefore not surprising that some experts have even argued that there is “no independent evidence whatsoever that the blacklisting technique has any significant effect on limiting terrorist financing” [12] and pointed out that the current “political statement” blacklisting approach can actually make the task of tracing money flows more difficult. According to Fitzgerald, this is because of a) the prevailing uncertainty regarding the details of the controls; b) the obligations the sanctions impose, and c) the manner of the sanctions enforcement. Importantly, a key shortcoming in all three areas lies in the lack of appreciation of the role of the private sector and its compliance with FTF measures:

[Reflections reflecting their origins as foreign policy tools, sanctions programs are often written quite broadly … for all transactions with blacklisted parties involving even the smallest amount or account. … Ironically, the result of broadly written controls is not wider compliance. Rather, those outside of the financial institutions at the core of the controls, recognizing that governmental enforcement resources are limited, may not engage in a high degree of “voluntary” compliance with what they perceive to be commercially impractical requirements. [32]

Alternatively, as Favarel-Garrigues et al. pointed out in their study of the French banks’ role in FTF, the term public-private partnership frequently used by public officials “seems somewhat inappropriate for defining relationships between banks and law enforcement agencies. It should be borne in mind that banks have been forced to comply with AML/FTF policy, and that the ‘partnership’ was clearly imposed ‘by command’ – that is, by the government.” [21]

**Squaring the Circle: Security and/or versus Profit?**

The final, yet arguably most daunting challenge, of public-private partnerships in the fight against terrorism stems from the difference of the very nature of public and private actors: “Businesses exist to provide a product or service in exchange for fees, thus producing profits. Governments also exist to provide services but also enforce rules, maintain order, and ensure well-being of the people.” [39] As a consequence, it is important to stress that although private and public actors nowadays have to interact in the security space, important difference remains between their primary interests: “The latter does not want to spend much time investigating and reporting suspicious transactions since their objective is to make profit. From a short term business perspective strict controls represent extra costs and refusing certain clients make them lose money.” [67] In other words, when it
comes to FTF, private institutions face what could be called a profit versus security dilemma. This is very apparent from the case study of FIs in the fight against terrorism, which highlights that they are primarily geared towards making profits and neither the origin nor the ultimate use of customers’ money has traditionally been of great interest to them. Demands and sanctions therefore indeed have to be placed on FIs:

[T]o overcome their natural reluctance to make too many problems for depositors, and thus kill the ‘golden goose’. At the same time, it is evident that financial institutions must engage in a large degree of self-policing for the monitoring to work properly. Where they are worried that they may themselves have breached difficult-to-follow and overly demanding legal requirements (especially as regards blacklists) they are not going to report themselves. [34]

As a consequence, as profit maximizing entities, FIs face a trade-off: they can either report less, thereby saving the costs to make all the reports for the FIU but accepting the possibility to get sanctioned, or they can increase the amount of reporting to decrease the chance of getting sanctioned, but having to accept the extra costs related to the production of extra reports.

As already discussed in the preceding section, within the current public regulatory framework, FIs have overwhelmingly opted for the latter option. To a large extent, this is because unlike size of the actual risk of terrorist financing in the financial sector, the costs of (non-)compliance with the FTF requirements are already well known and substantial. For example, the Peterson Institute of International Economics estimated the gross financial costs of the US anti-money laundering regime for 2003 at $7bn ($25 per capita): government/public sector $3bn; private sector compliance $4bn, general public (costs passed on by the private sector) $1bn. [52] Alternatively, a 2004 Swiss study found that AML measures account for 45 percent of the total regulatory burden and 2 percent of the total costs in Swiss private banking. [52] Specifically, FIs incur direct expenses by “establishing and maintaining risk management and compliance systems, the prospect of reduced income as a result of decisions to forgo certain lines of business, costs that might be associated with the possible diversion of resources from other aspects of the bank’s work, and the more intangible, yet important costs of inconvenience to customers.” Even more importantly, however, FIs face various potential costs, which include “civil and criminal monetary penalties, other sanctions such as cease and desist orders, or the removal of
management, the loss of some lines of business and reputational damage which can result in a loss of business.” [35] The available evidence suggests that the latter type of costs can be so substantial that they can bring into question not only the company’s share price and customer base, but its very existence (see table 2). This concerns especially the small banks, because “the cost FTF of regulation exhibits strong economies of scale.” [26]

[Table 2 somewhere here]

In light of the substantial penalties for non-compliance with FTF measures, it is not surprising that much of the available literature suggests that “banks are merely going through the procedures as evidence of compliance rather than in the expectation of unearthing criminal activity.” [30] Although a few studies have argued that large FIs can actually derive tangible benefits from their compliance with the CFT requirements, such as the development of sophisticated customer databases that can be used for marketing tools or the development of new products, [48, 61] the majority of experts agree that in addition to the fear of penalization from public authorities, FIs investments in FTF measures serve one primary goal – reputation protection: “[T]he reputational risk (and following from this, the impact on profit-making) has become too high to take. ... Banks chose to intensify their checks and procedures, as any association with terrorism financing could have disastrous effects.” [64] It is important to note, however, that although the FTF framework requirements are designed in a way that inevitably provokes fear of penalties and reputational damage, “this fear does not automatically mean that reporting institutions will provide higher quality intelligence to the authorities in a consistent and methodical way, because the system is largely based on vague concepts and subjective assessments.” [27] Moreover, FIs are only fined for false negatives, i.e. for not reporting transactions which are later prosecuted as money laundering or terrorist financing judged to be suspicious ex-post. In contrast, they are not fined for false positives, i.e. for reporting legal transactions as money laundering or terrorist financing.
Broader Implications for the Public-Private Partnerships in the Fight against Terrorism

The case study of public-private partnerships in the fight against terrorist financing also challenges several plausible remedies to the shortcomings of PPPs in counterterrorism. The first is based on the argument that the traditional concept of corporate social responsibility can be extended to include security, because in the post 9-11 era, “security is not a right that each of us possesses but rather a duty that everyone is responsible to uphold.” [50] The behavior of financial institutions within the existing FTF frameworks, however, suggests that private sector actors may take certain security risks simply because it is more profitable than actually addressing them. This is due to the fact that private sector actors actually have four options when it comes to addressing particular security threats, including terrorism:

1. Accept the risk of the threat’s actual occurrence, as the costs of countering it may be greater than the potential benefits.
2. Transfer the costs related to threat’s actual occurrence, which is usually done with purchasing an insurance policy.
3. Minimize the risk of the threat’s actual occurrence by adopting a wide range of measures such as new security policies and procedures, staff training, disaster recovery procedures, physical and logistical controls etc.
4. Terminate activities that are most threatened to eliminate the risk of the threat’s actual occurrence all together. [39]

Some authors have nonetheless suggested that option three – which is the only one available to public agencies in matters of national security, where actions are generally based on the precautionary principle of “better safe than sorry” – could also be made more attractive to regular private businesses under the rubric of corporate social responsibility by employing negative as well positive incentives. While the former approach implies stricter regulation and penalties as in the case of FTF, the latter approach is based on various tax incentives or specific security-related grants provided by public authorities. Other experts have made the case for option two from the aforementioned list by suggesting that private companies ought to see the fight against terrorism and their corporate security expenditures as a form of insurance, because after all, “[e]veryone buys car insurance, home insurance, life insurance, and short-term disability policies.” [39]

The case study of the fight against terrorist financing, however, shows that in practice, private sector actors make decisions about their investments in
security based on “(1) what is known about the risk environment, and (2) what is economically justifiable and sustainable in a competitive market place or in an environment with limited resources.” [39] While statistics differ from country to country, the probability of a particular private business becoming a target in a terrorist attack is almost everywhere much smaller than the probability of occurrence of the usual security risks that are commonly subjected to insurance policies. Moreover, in case of counterterrorism, we do not even have the data to make individualized risk assessments regarding particular types of terrorist threats. It is therefore not surprising that even under the threat of relatively severe penalizations, at least some private businesses will take the risk of not spending anything, or at least enough from the public authorities’ perspective, on counterterrorism measures. Perhaps most importantly, however, the case study of FTF also shows that it is precisely the notion of penalties and the reputational costs associated with being accused of not doing enough to fight terrorism that, from the private sector perspective, turns public-private partnerships into a one way street where public authorities direct in the traditional hierarchical mode of governance while also expecting that the cost of providing security will be born by the private sector.

Unsurprisingly, such notions of public-private partnerships are bound to look a lot like public-private dictatorships to most private businesses, whose representatives have traditionally been concerned about safety, rather than security:

Although both safety and security issues are considered to be corporate risks … safety is closely associated with the risk that the company chooses to run while security involves the threat the company is exposed to. … As regards safety, it is the company itself – its internal management and production – that is identified as the source of both the problem and the solution. Safety is therefore conceptualized as a relatively technical and controllable problem … Security, on the other hand, deals with human intentions. Security is an external threat – a matter of interference – and therefore appears less controllable. [50]

Some authors have recently coined an all-hazards approach to dealing with contemporary security threats, including terrorism, which blurs this traditional distinction between safety and security by referring to a generic notion of a

---

15 According to one recent British study, “[i]n quantitative terms, the risk of falling victim to a terrorist attack was 33 times smaller than dying of meningitis, 822 times than being murdered for non-political reasons and 1,833 times less likely than being killed in a car accident.” [20]
complex emergency, in which threats may emerge anywhere, any time and with various consequences for both public and private sector actors. [14, 53] Nevertheless, notwithstanding the seemingly never-ending definitional debate, terrorism has always been conceptualized as a political risk and since “politics is external to the company, and the company does not take part in the creation of politics, … [it] can therefore not be considered responsible for risks or political developments. [50] In other words, since terrorism is defined as being outside the control of the market, private sector actors cannot manage it in the same technical manner as standard safety issues, such as credit card fraud. This suggests that regardless of the amount of public incentives, it will be extremely difficult to persuade private companies to adopt new security, rather than traditional safety, measures in the fight against terrorism, which they continue to perceive as a non-safety issue and non-traditional risk that ought to be primarily taken care off by the government(s).

Finally, in the literature on security privatization, it is possible to find arguments about emerging trends towards individualization and marketization of security, which in turn also lead to responsibilization of all private actors for its provision: “Responsible individual and corporate behavior entails installing burglar alarms and surveillance systems, engaging the services of a security company, participating in neighborhood watches, and other forms on non- or quasi-state-related security behavior.” [2, 41, 46] A similar argument is sometimes also presented in the literature on risk-based security approaches, which suggests that risk is no longer:

[S]imply a synonym for danger; it is a particular way of thinking about and responding to potential dangers. It is preventative, not restorative. Primarily actuarial and calculative, it works by designing and controlling spaces, through the collection of statistics and the production of categories of danger, and by surveillance. Risk is, therefore, a way of approaching security that can be deployed by private actors just as effectively as by public ones. [1, 18].

Combined together, the trends towards greater individualization and marketization of security and the ascendance of risk-based and responsibilization security logics have challenged the traditional understanding of security as a public good. [38] As such they may also be interpreted as supporting the idea of private sector actors naturally choosing option three, e.g. taking direct action against contemporary security threats, including terrorism. Nevertheless, as the case study of the fight
against terrorist financing suggests, not everyone is necessarily convinced that this is the best way of looking at contemporary security threats. Although some authors have contented that the current counterterrorism practices are expressions, as well as causes, of the breakdown of the traditionally central distinctions between the public and the private, [18] in the fight against terrorist financing both private financial institutions and relevant public authorities are acutely aware of their differences and most of the FI’s representatives would also prefer to keep the distance the public and the private as far as possible. Moreover, even though security today may well be a commodity that can be sought and bought sold on the free market, which has opened the way for a range of private security companies to actually sell security services and products as their main line of business, [2, 38] the vast majority of private sector actors still make profit by selling goods and services that have little to do with security in the traditional understanding of the term.

**Concluding Remarks**

The findings presented in the previous sections of this article suggest that at least in the area of the fight against terrorist financing, the idea of private-public partnership does not represent the best way to engage the private sector actors. Firstly, although they require execution by private sector entities, the existing measures to fight terrorist financing are based on the logic of risk assessment, which is rather problematic when it comes to the threat of terrorism that is extremely difficult to quantify for individual financial institutions. Moreover, the public authorities have provided the private sector with only vague clues for detecting customers and/or transactions that may be linked to terrorist financing, while demanding that financial institutions put in place elaborate and costly surveillance mechanisms and procedures.

Secondly, one of the key goals of all public-private partnerships – information sharing facilitation – has been hampered by the persisting lack of trust between the public and private actors, which in itself represents a pre-condition for successful cooperation among any type of actors. In addition to the fact that the two main models in the fight against terrorism themselves have been based on a number of assumptions about the nature of terrorist financing that may not be
warranted for many contemporary terrorist groups and some of their provisions are legally contentious, it appears that many public agencies still operate in the old mindset of hierarchical governance, erroneously expecting the private actors to take all necessary steps to fight terrorism regardless of their costs.

Thirdly, the hitherto experiences with the fight against terrorist financing also suggest that it is one thing for political elites to make public promises on the measures that need to be taken to fight terrorist finances, and quite another thing for them to persuade the relevant private financial institutions, over which politicians exercise only little control, to comply. In case of the fight against terrorist financing, private sector compliance has ultimately been secured with a combination of financial penalties and resulting reputational concerns. The problem is that private financial institutions have in response resorted to the practice of defensive compliance with the public regulations by (over-)reporting. This efficiency has, however, further diminished the already dubious effectiveness of the measures to fight terrorist financing, which is the exact opposite of what the public-private partnerships were expected to deliver.

Fourthly, it should be kept in mind that private entities are primarily profit, rather than security, maximizers. In the long run, this is arguably the single biggest challenge to all public-private partnerships in the fight against terrorism. Unlike the other aforementioned challenges, it cannot be fixed by improving the data and methodology, or by enhancing the information flow, which may over time also generate a modicum of trust between the relevant public and private sector actors. As a consequence, when it comes to dealing with contemporary terrorism, at least some private sectors actors are likely to pursue different options than the public agencies, which are expected and tasked with ensuring the maximum level of security possible.

Since 9/11, however, many regular private businesses have also been tasked to perform several security functions due to the continuous introduction of new legal and technical regulations by public authorities at both national and international level within the framework of the fight against terrorist financing. As such, the use of the term **public-private partnership** in this area of counterterrorism appears inappropriate because PPPs require “a complementarity of goals, mutual trust, clear goals and strategies, clear distribution of risks, clear sharing of responsibilities and authority, and market- and success-oriented...
thinking.” [19] Few, if any, of these preconditions have been met in the context of the fight against terrorist financing, primarily because for the public authorities, PPPs in this area of counterterrorism are perceived as security, rather than efficiency, enhancers.

Further case studies are therefore necessary to provide evidence of genuine PPPs in other areas of counterterrorism. Nevertheless, as long as a substantial part of counterterrorism rests on the shoulders of regular private businesses, for whom security provision usually implies at least some loss of profit, one can predict that the public-private partnerships will not represent some ideal middle option on a public-private continuum. As such, rather than the blurring between the public and the private, or security and safety, the real challenge seems to be in finding the right mix for particular areas of counterterrorism as it is clear that a fully public option is rarely plausible in the context of modern market economies while at the same, counterterrorism is still considered too important of a security issue to be left entirely in the hands of the private sector. This confirms an old adage that there are no easy ways of combating terrorism. But it also suggests that a marriage of convenience may well be the maximum one can reasonably hope for when it comes to the search for proper roles and relationships among public and private actors in the fight against terrorism.

References


Table 1: Number of Suspicious Activity Report Filings by Year in Selected Countries

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Belgium</td>
<td>2,183</td>
<td>3,926</td>
<td>5,771</td>
<td>7,747</td>
<td>13,120</td>
<td>9,953</td>
<td>11,234</td>
<td>10,148</td>
<td>9,938</td>
</tr>
<tr>
<td>Germany</td>
<td>3,282</td>
<td>2,935</td>
<td>3,289</td>
<td>NA</td>
<td>8,261</td>
<td>6,602</td>
<td>8,062</td>
<td>8,241</td>
<td>10,051</td>
</tr>
<tr>
<td>France</td>
<td>684</td>
<td>866</td>
<td>902</td>
<td>1,213</td>
<td>8,719</td>
<td>9,019</td>
<td>10,842</td>
<td>11,553</td>
<td>12,047</td>
</tr>
<tr>
<td>Netherlands</td>
<td>3,546</td>
<td>2,994</td>
<td>2,572</td>
<td>NA</td>
<td>24,741</td>
<td>37,748</td>
<td>41,003</td>
<td>38,481</td>
<td>NA</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>15,007</td>
<td>13,170</td>
<td>16,125</td>
<td>14,148</td>
<td>56,023</td>
<td>94,718</td>
<td>154,536</td>
<td>195,702</td>
<td>213,561</td>
</tr>
<tr>
<td>United States</td>
<td>NA</td>
<td>NA</td>
<td>62,473</td>
<td>81,242</td>
<td>281,373</td>
<td>507,217</td>
<td>689,414</td>
<td>919,230</td>
<td>1,078,894</td>
</tr>
</tbody>
</table>

Source: [27]. Data based on FIUs annual reports. Includes reports related to both money-laundering and terrorist financing.

Table 2: Examples of Banks Fined for AML/CTF Non-Compliance

<table>
<thead>
<tr>
<th>Bank</th>
<th>Date</th>
<th>Penalty and its justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>HSBC (UK)</td>
<td>2012</td>
<td>Fined $1.92 billion for money-laundering and sanctions-busting by US authorities.</td>
</tr>
<tr>
<td>Standard Chartered (UK)</td>
<td>2012</td>
<td>Fined $667 million for money-laundering and sanctions-busting by US authorities.</td>
</tr>
<tr>
<td>ING (Netherlands)</td>
<td>2012</td>
<td>Fined $619 million for money-laundering and sanctions-busting by US authorities.</td>
</tr>
<tr>
<td>RBS (UK)</td>
<td>2010</td>
<td>Fined $500 million for money-laundering and sanctions-busting by US authorities.</td>
</tr>
<tr>
<td>Barclays (UK)</td>
<td>2010</td>
<td>Fined $298 million for money-laundering and sanctions-busting by US authorities.</td>
</tr>
<tr>
<td>Credit Suisse (Switzerland)</td>
<td>2009</td>
<td>Fined $536 million for money-laundering and sanctions-busting by US authorities.</td>
</tr>
<tr>
<td>Lloyds Banking Group (UK)</td>
<td></td>
<td>Fined $350 million for money-laundering and sanctions-busting by US authorities.</td>
</tr>
<tr>
<td>ABN-AMRO Bank (US)</td>
<td>2005</td>
<td>Fined $80 million for failing to implement an effective anti-money laundering program.</td>
</tr>
<tr>
<td>Arab Bank (Jordan)</td>
<td>2004</td>
<td>Fined $24 million for failing to implement an effective anti-money laundering program by US authorities.</td>
</tr>
<tr>
<td>AmSouth Bank (Netherlands)</td>
<td>2004</td>
<td>Fined $50 million for failing to implement an effective anti-money laundering program by US authorities.</td>
</tr>
<tr>
<td>Commercial Bank of Syria and its subsidiary Syrian Lebanese Bank</td>
<td>2004</td>
<td>Designed as “financial institutions of primary money laundering concern” by US authorities, no business with US FIs.</td>
</tr>
<tr>
<td>Riggs Banks (US)</td>
<td>2004</td>
<td>Civil penalties $25 million and criminal penalties of $16 million for failing to implement an effective anti-money laundering program. Later taken over by the PNC bank.</td>
</tr>
<tr>
<td>Citigroup (US, Japanese branch)</td>
<td>2004</td>
<td>Ordered to close its private operations due to concerns about failure of AML internal system controls by Japanese authorities. The value of the company’s shares declined by 2.75 percent the week following the announcement.</td>
</tr>
<tr>
<td>Bank of Scotland (UK)</td>
<td>2004</td>
<td>Fined £1,250,000 for failing to keep customer identification records to the required standard by UK authorities.</td>
</tr>
<tr>
<td>Abbey National Bank (UK)</td>
<td>2003</td>
<td>Fined £2,320,000 for failures to comply with existing anti-money laundering regulations by UK authorities.</td>
</tr>
<tr>
<td>The Northern Bank (UK)</td>
<td>2003</td>
<td>Fined £1,250,000 for failures to comply with existing anti-money laundering regulations by UK authorities.</td>
</tr>
</tbody>
</table>

Sources: Author’s research.
Figure 1: Cumulative Worldwide Amounts of Frozen Terrorist Assets, 2000-2008