TERRORISM AND BUSINESS

Speaking Notes for Alyson JK Bailes, Director, SIPRI
Groupe d'Économie Mondiale, Sciences-Po, Paris 5 September 2006

Introduction

The second time I attended the Davos World Economic Forum, in January 2004, I heard a presentation on Al-Qaeda by an American expert where he argued that the best way to think about it is as a global franchise, like Macdonalds. Just as with Macdonalds, Al-Qaeda has become a brand-name instantly recognizable anywhere. It has a limited range of products that can be reproduced with local raw materials in just about any part of the world. It typically employs young people who have trouble taking other jobs because of lack of skills or ethnic origin or possibly something in their attitude. And it is so popular that it ends up being imitated, especially in less developed parts of the world, to such a point that it is often hard to say what products and activities have been approved by the central Macdonalds authorities and which have not.

Since the expert in question came from the USA this comparison was clearly not meant just as a joke. It was trying to make the serious points that (i) the methods of organization of modern terrorism are very different from those of a traditional government structure, or even a traditional civil society organization; that (ii) such models as we have for them may best be found among the latest permutations of commercial business activity; and (iii) – by implication – that business experts might be able to do more than a little to help government experts in understanding and countering them. That last thought is also where my talk to day is going to end up; but before I get there, I would like to talk through two other aspects of the relationship between terrorism and business in a bit more detail:

- first, to what extent is business itself (and especially its 'darker side') part of the problem, as a *source* or a *habitat* or an *accomplice* for terrorism;
- secondly, the notion of business as a *target* or *victim* of terrorism;

- and then I can come back finally to the idea of business as part of the solution, as a *partner* against terrorism.

Business as Part of the Problem

It has become almost a cliché of analysis that genuinely 'transnational' terrorists of the Al-Qaeda type, or even many of those who fight for more specific political and geographical causes, do not operate in the classic Westphalian space of inter-state warfare and diplomacy. It is possible to think of their environment instead as a kind of global social space in which individuals of all backgrounds can act and affect each in other in new ways both as attackers and as victims; but it is equally logical and relevant to think of terrorists moving within the new globalized dimension of the *private, civilian economy*. Their funds may come from private wealth, from donations channelled through private banks and the Islamic world's more informal and personalized 'Hawala' system; from illicit trading for instance in diamonds and drugs and other forms of smuggling, or from human trafficking and prostitution; from robbing banks and other forms of theft, or from other proceeds of criminal activity like protection rackets. Plain and simple economic corruption, notably in the form of bribes to individuals, is one of the commonest ways by which terrorists obtain information and supplies, and manage to cover up their activities. Their weapons and other equipment may also be obtained through illicit trading deals by governments or non-governmental players, or by simple purchase on the market given that bombs (for instance) can be put together from many everyday ingredients. The globalized environment with its massive and varied flows of human travel, goods circulation and communications provides an ideal setting for terrorists to travel for consultations, fund-raising and training as well as for planning and carrying out their attacks. The large 'black' and grey' economic markets that exist in many countries, and their connection with labour sources of equally fuzzy status like illegal immigrants and moonlighting workers, help to create the habitat in which terrorists can not only move from nation to nation but 'go underground' within a particular society. Last and not least, the global IT networks that help terrorists to collect and exchange information, and the media establishments that they rely on to publicize their exploits, are today commercially owned if they are owned by anyone.

The USA's National Security Strategy of September 2002 stated that the biggest threat to the American people today 'lies at the crossroads of radicalism and technology', and whatever we may feel about the rest of the Strategy, that remark is one I find quite intellectually satisfying. It is true not just in the sense that terrorists attain their greatest destructive power by exploiting the highest technology, but also in the sense that many of the same features of the globalized economy are tending to aggravate both sides of the problem. You will recall that the Secretary-General of the International Atomic Energy Authority (IAEA), Mohamed El Baradei, talked about a 'Wal-mart' of nuclear smuggling following the revelation of how Pakistani scientist A.Q. Khan had spread his nuclear secrets abroad: and the image was a good one not just in implying a big shop where almost anyone could buy anything, but also because it hinted at the mercenary nature of many of the motives involved. Even if Khan himself was driven by higher things than profit, the middle-men he used in such varied locations as Dubai and Malaysia - and those who were discovered during the similar post-mortem on Libya's nuclear ambitions after Qhadafi gave up his WMD programme—were part of a single shady establishment that is liable to be involved in many other kinds of illicit goods and money transfers. The same can be said of the contexts in which various attempts to trade nuclear materials originating from programmes in the former Soviet Union have been unmasked.

This connection with the 'black' or 'grey' market is, however, only one part of the total interface between the private sector and the risks of WMD proliferation. At least when we are dealing with cases of nuclear smuggling to terrorists it is pretty plain where the problem to security starts and that we are dealing with activities outside the law. A far greater challenge is that all the techniques involved in WMD development—the harnessing of the atom, synthetic chemical production and the human creation and use of biologically active organisms or substances—have their main and quite legitimate use in the sphere of the civilian economy. The processes that produce nuclear weapons and civil nuclear energy respectively go along different tracks in their later stages, but they both use the same fissile materials (uranium and plutonium) and start off with many of the same initial processes and equipment – which is what complicates the challenge of dealing with cases like Iran and North Korea. Besides, as we know, terrorists could also use relatively 'innocent' products, including medical isotopes, to set off so-called 'dirty bombs' (radiological weapons) that release radioactivity in a social setting and which are likely to be especially damaging in terms of economic losses caused.

In the fields of chemical and biological weapons (CBW) it is hard even to be sure what a 'weapon' is. Governments making chemical weapons have favoured certain limited combinations of chemicals from the early twentieth century towards, and these substances are certainly among those that terrorists might try to mix for themselves or to acquire through the black market, as Aum Shinrikyo used Sarin gas for its attack in the Toko subway; but many other everyday chemicals have explosive, corrosive, poisonous or otherwise destructive effects that terrorists might equally well exploit with generally less danger to themselves. The scale of the problem will be clear enough if you think of the human and economic damage done by the industrial chemical accidents at Seveso in Italy and Bhopal in India, or by accidental industrial releases of mercury in parts of Japan. Similarly, governmental experiments to develop biological weapons and ways of delivering them are believed to have focussed on a relatively few historic diseases including anthrax, small-pox and varieties of plague; but the range of bio-substances that could cause massive human damage if used by terrorists is just as wide as or wider than those that can hurt humans 'naturally' or by accident—any kind of disease organism, any organic poison or contaminant, any pest affecting animals and crops or making water undrinkable, and so on. Even antidotes, cures and protection techniques could be misused for offensive purposes, if terrorists could use them to protect their own people while releasing the corresponding bio-hazards into the environment. All this is without mentioning the mass destruction potential of techniques that are still in the early stages of commercial development like genetic manipulation and nanotechnology.

To make clear how this fits with our main theme, I should stress that the environment where these technology-related risks arise is today overwhelmingly a private sector, free-market one. Privately owned companies not only produce and operate nuclear, chemical and bio-industrial equipment but today carry out by far the greatest share of the basic scientific research and development for the relevant technologies, goods, and methods of application. Even university research is often commercially funded, and even governments themselves are tending more and more to explore various forms of 'public-private partnership' for high-tech research, development and production, not excluding the field of defence and even of WMD. (The British government was considering recently even putting its nuclear safety inspectorate into private hands). It is private companies who produce nuclear power, as well as things needed to confront the nuclear danger such as radiation monitoring equipment and iodine tablets; it is they who produce both poisonous gases and gas-masks; it is they who identify or artificially create new strains of disease, as well as producing the masks and gloves, the pharmaceuticals or bio-active cures that are needed to counter them.

I hope all this is enough to have started convincing you already that we do not have much of a hope of finding effective defences against the misuse of all these objects and technologies by terrorists, or indeed by anyone else, unless we can win the active involvement and cooperation of the private sector itself. Before turning to that, however, let's consider whether the private sector has a practical interest of its own in combating terrorism, and if so for what reasons.

Business as Victim

The first and simplest answer is that business itself has provided many of the targets for terrorism and many of its victims, not just in New York on 9/11[1] and since then, but throughout much of the twentieth century. When terrorists are animated by political and ideological agendas, they may choose to include business premises and personalities among their attacks because they are

- soft targets (less well protected)
- profitable targets (in the case of kidnapping and extortion)

[1] The majority of direct casualties that day were commercial employees and one single commercial law firm, Cantor Fitzgerald Securities, lost approx. 700 out of 1000 employees.

- symbolic targets, symbolizing the economic strength of the state as the Twin Towers did, or symbolizing modern capitalism when that is part of what the terrorists object to.

In addition, however, business is the original and direct target for those widespread varieties of terrorism whose anger is directed at things business itself does, such as eco-terrorism, or the violent wings of the anti-abortion movement and animal rights movement when they attack private clinics and laboratories.

It is also clear [and has been discussed in the (other/earlier) presentations today] how business is affected by the direct side-effects of a terrorist attack: some companies may indeed get new building contracts, but the insurance industry always suffers heavy losses, and any larger-scale event like 9/11 or the bombs in Bali, Madrid and London leads to a temporary drop in tourism and in the revenues of the transport sector and entertainment sector. Transport companies and perhaps others are also hit by raised insurance premiums, which became such a huge problem for aviation after 9/11 that governments had to step in as guarantors of last resort.

Then there are the burdens created for business by deliberate government actions, and those of intergovernmental organizations, that are taken in response to terrorism to punish the people considered to be responsible or to make further attacks more difficult. In the category of punishment measures come trade sanctions, bans on airlines and similar embargoes that affect business with individual countries. The range of preventive and defensive measures has become much wider especially since 9/11 and can include:

- new legal codes that create obligations for business and private citizens as well as states: the most ambitious examples are the global prohibition of terrorist financing and the ban on unauthorized possession and trading of WMD that were created by the UN Security Council Resolutions 1373 and 1549 respectively;
- more specific measures to limit the transfer, including through private business channels, of particularly sensitive items and technologies, and to make access to and the theft of such things more difficult for terrorists as well as for other criminals and for irresponsible states. In the case of terrorism the items of concern include all WMD-related materials but also for instance missile technologies and man-portable anti-aircraft weapons (MANPADS). Many steps to widen the range of such controls and enforce them better have been taken since 9/11 by the various multilateral export control groups made up mainly of Western nations, but we could also add the new efforts made in the G8, IAEA and elsewhere to control the management of civil nuclear fuel cycles, to improve the physical security of civil nuclear and other sensitive installations, and to speed up the destruction of surplus WMD-related materials;
- measures to forcibly stop the physical transfer of suspected items, namely the Proliferation Security Initiative launched by the USA and France among others in 2003 and which has as its most dramatic feature the possible forceful interception of ships at sea;
- enhanced measures for aviation security and for the security of ports, harbours, container traffic and ships, which – as we have just seen in the UK – can involve losses quickly mounting into millions and billions of Euros when they involve actual cancellations, but which always inflict some generic rise in companies' operating costs as well as extra delay, hassle and probably expense for business travelers;
- tighter controls on the issuing of visas and immigration procedures generally.

The great majority of these official measures in the last five years have been made without any advance consultation with business; and while responsible business leaders have seen some genuine value in them, as ways of protecting respectable commerce against crime and smuggling as well as terrorism as such, there have been growing complaints even within America about the excessive or unfair burden of the *cumulative* costs. Business complaints have been particularly loud about the USA's new visa and travel rules which are making it almost impossible to do business with customers from certain countries or to recruit scientists and other employees from among them. This helps to explain why, although the direct threat from terrorism has always had to be taken seriously especially by the larger global companies, many such companies would now see the risk of excessive and ineffective government action against terrorism as actually *more* of a danger to their business and their profits than the damage done by the terrorists themselves.

The most risky action taken by the USA and some of its allies has of course been the military invasion of Afghanistan to tackle Al-Qaeda, and then the invasion of Iraq where Iraqi support for terrorism was mentioned as a secondary motive after the WMD threat - if never very convincingly. It is notorious that certain companies from the USA and to a lesser extent the UK have received extremely profitable contracts, especially in Iraq, not just for the kind of short-term humanitarian supplies and rebuilding that you would expect private business to help with in any conflict, but also for security-related services going right up to armed combat and the guarding of prisoners. It is easy and probably right to be cynical about this kind of private-sector profiteering out of the terrorism issue; but what I want to stress here is that the same situations that benefit a few companies like Halliburton are causing a much wider range of problems for a much larger number of 'normal' companies, including those who would like to help get Iraqi trade and industry going again but find it impossible to operate normally there because of the continuing chaos. Even the political fallout from the Iraq affair has affected businesses on both sides of the Atlantic, at the time when there were attempts at boycotts on French goods in the USA or vice versa. My overall conclusion from all this is that for the great majority of companies, both terrorism and the violent official reaction to terrorism are inherently *unprofitabl*e: and that the balance of the account becomes even more negative when tertiary economic effects like the rise in price of oil-based energy inputs are taken into account. There should therefore be a prima facie commercial interest in helping governments to find better solutions and to enforce them also in commercial and private contexts, not least to protect the companies themselves and the consumers whose money they rely on.

Business as partner

How to use business better as a partner against terrorism is not the hardest part of the question. Private expertise and competence can be drawn upon in 3 generic ways at 3 stages of policy formation:

- in the analysis of threats and risks, especially in locations where business has deep experience of security dynamics and can maintain contacts that might be impossible for the corresponding governments; also as I mentioned at the outset, help in understanding the very nature of terrorist 'franchises'
- in the design and drafting of policy instruments that deal directly with market operations, such as export controls, financial regulations and measures of transport and infrastructure security, and other measures that may have major economic impact such as those in the nuclear industry

- in the execution of such measures at the company and individual level, which should include reporting back on their effectiveness and helping to refine them through experience.

Just as no single government can effectively grip the problem on its own, this interplay with business needs to take place not just at the national level but also at the level of regional and global organizations. Moreover, given the origins of many terrorist movements and the truly global nature of the dimensions in which they operate, there is little point in recruiting just a limited number of supposedly well-behaving Western companies to help unless some way can be found of engaging also with the businesses of Southern hemisphere regions and especially of the largest emerging markets. (The growth of 'outsourcing' to these countries, sometimes involving the delegation of functions and services that are quite important for security, provides yet another argument for this.) The government of Dubai recently allocated a million dollars for trying to improve its defences especially against the smuggling and transit of sensitive goods and has explicitly mentioned the need to reform business practices in this connection, which shows that the point can at least be well understood in non-Western environments.

Even in the West, however, the problem is often that even if governments did decide to work with business it is not always clear what their contact point or method of communication would be. My last suggestion is therefore that business itself needs to think about organizing itself in new interest groups, or making using of existing structures like chambers of commerce, employers' federations and sectoral associations, to offer an efficient 'homologue' for communication with government and to find the best way of preparing and harmonizing its own positions on this whole range of issues. One idea I have suggested is that some like-minded large companies could consider developing a doctrine of 'Corporate Security Responsibility' along the same lines as the existing Corporate Social Responsibility, and that the doctrine should start with emphasizing what businesses need to do and can do for their own security against terrorism (among other things), before going on to measures that they should take to avoid causing or conniving in security problems, and the part they could play in helping other authorities to get the problems under control. The beauty of capitalism is that if a clear code of this sort existed and some businesses were seen to get approval and profit for following it, the market itself ought to make more and more others imitate them.