14. The security of business: a view from the security industry

Crispin Black

I. Introduction

Private security companies have been in existence for a long time—at least as long as, or longer than, the modern concept of government's role in the provision of security. Just one example may be cited which is topical on both sides of the Atlantic at the time of writing in view of the visits of US President George W. Bush to London and Baghdad in the autumn of 2003. In 1861, while investigating a railway case in Baltimore, Maryland, the Pinkerton private detective agency uncovered a plot to assassinate President-elect Abraham Lincoln when he passed through Baltimore on his way to Washington for his inauguration. Allan Pinkerton himself warned Lincoln, who changed cars in the middle of the night for the final leg of his train journey.[1] A core of private security agents surrounding Pinkerton later formed the embryo of the US Secret Service and the forerunner to the Federal Bureau of Investigation.

Having laid the foundations in many parts of the world for police forces and intelligence agencies, private security companies subsequently passed on the primary responsibility to the state. In a nice historical irony, a significant part of these functions and responsibilities seems in the early 21st century to be drifting back to the private sector. Modern Western states need help in providing the security that their citizens want and need.

A typical modern security company provides services across a spectrum. Most companies have both an analytical/intelligence arm and a 'hands-on' physical security arm—usually operating in close concert. The physical security arm in a British company is normally staffed by former members of the military establishment, many with experience in the Special Forces. The types of service offered can further be subdivided into 'consulting services', where the security company acts as an expert adviser, and 'specialist security services', where the security company actually provides a physical service.

This chapter provides, in section II, further details of the range of services now available from the private security sector; it then discusses (section III) the historic interplay of governmental, private and military actors in security emergencies. It ends with some personal reflections on the United Kingdom's experience of intelligence gathering and assessment and on a possible new role for the private sector (section IV). Brief conclusions are presented in section V.

[1] On this incident see URL <http://en2.wikipedia.org/wiki/Allan_Pinkerton>.

II. The services available

The consulting services available from private security companies typically include the following types.

Security intelligence gathering. Private firms have a requirement to gather and then analyse intelligence to support either particular projects for clients or their own general operations. Such intelligence-gathering activities can be either defensive or offensive in aim. Some security firms also offer a general business intelligence service involving 'due diligence' searches prior to deals, mergers or acquisitions.

Threat assessment and security risk analysis. Security provision in the modern world requires a sound intellectual and conceptual basis. It is only through a thorough analysis of the threats and vulnerabilities facing a commercial enterprise that a plan can be put together to mitigate them. In view of the current globalized terrorist threat, the process of comprehensive security risk analysis—including projections of future risks—is being increasingly understood and used by private companies.

Security survey and audit. This process involves a detailed inspection of premises and staff activity in order to identify physical or electronic vulnerabilities. As part of such an audit, or separately, security companies can offer assessment and advice on information technology (IT) security and cyber risk management; security training (for those responsible for security and/or all personnel); help with contingency planning; and advice and help with security crisis management.

Penetration testing. This involves covertly testing vulnerabilities in security management systems, either by exploiting weaknesses in physical and information system security, or by exposing gaps in procedures and training of staff and contractors. Such tests, carried out by members of specialized security companies, allow company risk managers to understand the specific vulnerabilities in their systems by observing them being exploited.

Specialist security services typically include the following activities.

High-risk operations. This entails the provision of a full range of protective and training security services to allow a commercial enterprise to carry out its business in hostile circumstances. There is a worldwide requirement for this kind of service, particularly in the states members of the Commonwealth of Independent States (CIS)[2] and in the regions of Africa, Latin America and the Middle East. Currently, the companies helping to rebuild Iraq are mostly protected by private security companies.

Close protection. This service is increasingly in demand for the protection of key individuals or those carrying out necessary duties in particularly threaten-

[2] The CIS member states are Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Turkmenistan, Ukraine and Uzbekistan.

ing environments. In addition to 'close' bodyguarding skills, this service usually involves the gathering of protective intelligence.

Surveillance and counter-surveillance. Counter-surveillance in particular is becoming an increasingly important part of the private security business. Most serious crimes and nearly all terrorist attacks require some form of detailed reconnaissance in advance, which is usually apparent to a surveillance professional and often apparent to the layman with some surveillance-awareness training. British companies are particularly strong in this area because of the British military's extensive experience of counter-terrorism in Northern Ireland.

Employee screening. Screening programmes identify dishonest or incompetent candidates for employment and minimize employee-related risk.

Confidential investigations. When internal fraud or information leaking are suspected, security companies provide the human and technological investigative services required.[3]

III. Survival planning: never a state monopoly?

Survival planning is not new. The ancestors of those living in today's highly developed countries of Western Europe and North America took such activity for granted in a world that was much less predictable than today's. The effort to meet and mitigate risk runs deep in both business and human culture, and people have rarely if ever been able to devolve the whole responsibility for providing it upon the state. In early modern Europe, things were often the other way round: it was private finance houses that supported both independent merchants, and national leaders and their armies, against the costs of operation and the financial consequences of failure. The principles of prudent risk calculation were the same as today, as was the danger that the exceptional, odds-against event would bring calamity to even the best prepared societies. Typically, in modern circumstances as well as the past, it is a string of unrelated but cumulative unlucky circumstances that generates the worst disasters.[4]

New human and animal epidemic diseases are often reckoned among today's worst threats to orderly commerce and government and to 'human security' in general, but there is nothing particularly novel about such 'plagues' either. The recent experience of Hong Kong and several countries with severe acute respiratory syndrome (SARS) reminded the world that, within living memory, people in highly developed countries had to confront the threat and terrible effects of infectious disease. The scourge of poliomyeli-

[3] This listing stops short of combat and combat-related services, which are defined as the purview of private *military* companies.

[4] The merchant Antonio in Shakespeare's play *The Merchant of Venice* was nearly ruined by the effects of weather in the English Channel despite what many would still see as a sensible risk mitigation strategy. As the character Shylock commented in this play, Antonio had spread his investment over several different ships on different routes, but: 'ships are but boards, sailors but men' (Act I, Scene III, lines 15–20).

tis, for instance, was not eradicated in the western hemisphere until 1994, and even later in Europe.[5] Any person living and working in the British Empire would have encountered or suffered from an array of communicable diseases which had to be endured or managed without the benefits of antibiotics.

An earlier medical emergency in Hong Kong—the Plague of 1894—also has lessons which are relevant today. The Hong Kong government of the day struck a special medal for all those seen to have done signal service to the colony, and most of the medals went to officers and men from the King's Shropshire Light Infantry, a military regiment in the British imperial garrison. They had undertaken palliative and hygienic measures in an attempt to stop the ravages of the plague. This was at a time before antibiotics and even before doctors understood how the disease was transmitted but, crucially, after the Western medical community had begun to understand the importance of hygiene and antisepsis. Of the 300 men from the regiment involved in the operation, only seven died as a result.[6] We see therefore that people near to us in history were able to bring under control diseases which inspire the deepest fear today, armed only with courage, sound decision making and a good deal of disinfectant. The other point of the story—also relevant today—is the way in which local administration drew upon the resources of those most able to help, who happened to be military personnel stationed for quite a different purpose. Just as the private sector may today penetrate into areas of security provision formerly reserved for state organs, state assets such as armed forces may have a potential that is still largely unexplored for solving various acute problems of human and 'homeland' security.

Another apparently eternal principle is that one man's crisis is another's opportunity. At any point of crisis evolution when people feel a shortfall of security but still have money in hand, there are business opportunities to be seized by both responsible and unscrupulous traders. Modern examples would be the rush on gas masks, emergency supplies and private shelters after the events of 11 September 2001, or the lively and often controversial competition for reconstruction contracts after the occupation of Iraq in 2003. An older instance would be the Great Fire of London in 1666 and the observations of contemporary diarist (and business survival planner) Samuel Pepys. His diary entry for 5 September 1666 records a visit to an area just outside the city that was crammed with poor refugees who had lost everything. The diarist is deeply distressed by their plight and the damage to his beloved city, but his lamentations are cut short by the laconic entry 'paid two-pence for a plain penny loaf'.[7] The lesson is clear: survival planning can represent a business opportunity. Somehow, a baker had managed to keep producing his goods, and doubled his price in the process.

[5] See, e.g., the Internet site of the US Advisory Committee on Immunization Practices at URL <http://www.cdc.gov/mmwr/preview/mmwrhtml/rr4905a1.htm>; and the World Health Organization Internet site at URL <www.who.int/gb/EB_WHA/PDF/WHA52/ew8.pdf>.

[6] On the King's Shropshire Light Infantry consult URL <http://www.lightinfantry.org.uk>.

[7] Pepys, S., eds R. C. Latham and W. Matthews, *The Diary of Samuel Pepys,* vol. 7 (1666), (Harper Collins: London, 1995), p. 277.

IV. Terrorism and intelligence

Terrorism is not new—not even for the United States, although 11 September 2001 was a serious break from the past. Outsiders had not attacked the continental United States since the War of 1812, but the mindset and methods behind the attacks by Islamicists on that day changed the world in one crucial respect. For the first time since the 1962 Cuban missile crisis, the collection and analysis of intelligence became crucial to the safety of every man, woman and child living in the democratic West.

Although efforts for intelligence collection go back at least as far as the existence of organized states, it is only comparatively recently that this work has been understood and treated as a state monopoly. As mentioned above, private detection agencies were the ancestors of public ones in the USA, and in the UK there has long been a cultural predisposition for private individuals to become involved in this sector. During World War II, in the UK, the breaking of the German Enigma codes (used in one form or another for all military communications) was largely entrusted to a mix of civilians, university lecturers, crossword and chess enthusiasts, and clever undergraduates recruited by word of mouth[8] and brought together at Bletchley Park in Hertfordshire. In this heterodox environment, private individuals with no military background achieved brilliant success. The 'Double-Cross System'—the code name for a sustained series of operations which captured nearly every German spy despatched to the UK and then turned many of them into double agents—was the creation of Oxford don and detective novelist J. C. Masterman.[9] What such outsiders brought, and what the operation needed, was mental nimbleness, abilities unconstrained by standard training and a willingness to 'think outside the box'. Such qualities are still a necessary part of the mix for good intelligence work today.

After the war, in the UK the highest responsibility for intelligence assessment—carefully kept distinct from the business of intelligence collection—devolved upon the Joint Intelligence Committee (JIC), which had been created in 1936.[10] The members of the JIC, which is technically a sub-committee of the Cabinet of Ministers, are senior representatives of the Foreign and Commonwealth Office, the Ministry of Defence and other departments; the heads of the three intelligence and security agencies; and normally a representative of the Prime Minister's staff. The secretariat for the JIC is provided by the Cabinet Office Assessments Staff, manned by civil servants and military officers recruited from the whole range of government departments by open competition. This personnel structure was expressly designed to protect the JIC

[8] In late 1941 they were recruited through a crossword competition organized by *The Daily Telegraph.* Smith, M., *Station X: The Codebreakers of Bletchley Park* (Channel 4 Books: London, 1998).

[9] Masterman, J. C., *The Double-Cross System in the War of 1939–1945* (Yale University Press: New Haven, Conn., 1972).

[10] See Cradock, P., *Know Your Enemy: How the Joint Intelligence Committee Saw the World* (John Murray: London, 2002); and 'Iraq's chemical, biological, nuclear and ballistic missile programmes', URL <http://www.number-10.gov.uk/output/Page273.asp>.

and its staff from inbuilt bias towards any individual intelligence agency and from excessive interference from any policy-driven ministry. It reflects a traditional desire to keep the British civil service impartial and separate from elected politicians and their appointees—very different from the 'spoils system' prevailing in the USA, where the national security adviser is a personal nominee of the president. Through the national intelligence priorities which it sets, its overview of intelligence cooperation with other nations, and the analytical papers which it approves on the basis of drafts from the Assessments Staff, the JIC aims to provide to the Crown, ministers, the armed forces and senior officials an agreed and bias-free national assessment on weighty intelligence matters.

So far, so good in principle: but events since 11 September 2001 have brought the impartiality and efficiency of the British, as well as the US, national intelligence apparatus into question. In the first place, there is the issue of why these systems were unable to anticipate or warn of the attacks. The Joint Inquiry by the Senate Select Committee on Intelligence, and the House Permanent Select Committee on Intelligence, into the activities of the US intelligence community in connection with the attacks goes to the heart of the problem in its systemic finding number 5.

> Prior to September 11, the Intelligence Community's understanding of al-Qa'ida was hampered by insufficient analytic focus and quality, particularly in terms of strategic analysis . . . there was a dearth of creative, aggressive analysis targeting Bin Ladin and a persistent inability to comprehend the collective significance of individual pieces of intelligence. These analytic deficiencies seriously undercut the ability of U.S. policy makers to understand the full nature of the threat, and to make fully informed decisions.[11]

Criticizing intelligence failures with hindsight is, of course, easier than predicting events in the future or making sense of piecemeal intelligence. However, there was little sign that the lessons of September 2001 had been learned when, in a later phase of the crisis, British and US forces prepared together to defeat the forces of Saddam Hussein and to occupy Iraq. The question that the British and US intelligence establishments appear to have been asking themselves and answering at that stage was: how easy would it be to win the war? A more sensible question might have been: given that formal military resistance to a US-led combined arms offensive in Iraq would be both suicidal and ineffective, how will Iraqis who are loyal to Saddam Hussein (and others) seek to force the US allies out of Iraq after the war has been won? More serious reflection on this question, and on other worst-case contingencies, might have spared the occupying forces and the people of Iraq many of the unpleasant surprises that faced and still face them in the attempt to 'win the peace'.

[11] United States Congress, *Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001: Abridged Findings and Conclusions* (US Government Printing Office: Washington, DC, 2002), p. xvi.

This was not, by far, the only apparent failure of crisis-linked or terrorism-linked intelligence in modern times. The collapse of the Soviet Union, on which the bulk of the British and US intelligence effort had been focused, came as a surprise to most. Famously, in the history of the British intelligence community, the JIC failed to anticipate the Argentinian invasion of the Falkland Islands in 1982, despite clear evidence that it was in the offing.[12] Add this to the recent failures over Islamist extremism, and it might suggest that there is a cultural or organizational factor at work rather than any ad hoc reason for failure—or at the very least, that serious intelligence gathering and analysis operates at the edge of human intellectual and judgemental capabilities.

These concerns are deepened by the recent indications, also linked to the Iraq crisis, that the intelligence communities on both sides of the Atlantic may have come under irresistible political pressure to publish assessments that made the strongest possible case for a pre-emptive attack on Saddam Hussein. Whatever the final verdict may be on the extent of and responsibility for specific distortions of the evidence,[13] it already seems clear that Prime Minister Tony Blair and his advisers gave the JIC and its products a more 'instrumental' role than had ever before been thought proper in making their policy case to the nation. According to the accounts so far available, the Chairman of the JIC seems to have been too willing to accommodate the government's presentational and substantive concerns by allowing changes to the wording in a key document about Saddam's weapons of mass destruction (WMD) capability.[14] The episode has awakened serious concerns in all parts of the British political spectrum about the reliability of the present assessment system, the JIC's relations with the executive branch, and the larger question of the extent to which major state decisions involving the use of force can be based on intelligence alone.[15]

It need hardly be underlined that any actual or perceived weakening of the JIC system in the UK—or the intelligence equivalent in any Western state—is a matter of more than ephemeral political concern. The reliability of intelligence assessments is important not just for the success of the country's exter-

[12] West, N., *The Secret War for the Falklands: The SAS, MI6, and the War Whitehall Nearly Lost* (Little Brown and Co.: London, 1997), pp. 25–57, provides a full account of the role of the JIC before and during the 1982 Falklands/Malvinas War.

[13] An official enquiry under Lord Hutton was appointed to look into the circumstances surrounding the death of Dr David Kelly—a British civil servant who had been reported in the press as saying that an intelligence-based dossier had been 'sexed up' for public presentation—and the final report is still awaited at the time of writing. On the Hutton Inquiry see URL <http://www.the-hutton-inquiry.org.uk>.

[14] See Kampfner, M., *Blair's Wars* (Free Press: London, 2003).

[15] Former British Foreign Secretary Lord Owen was vituperative in his comments in a speech at the London School of Economics on 9 Oct. 2003: 'I do not need to await Lord Hutton's verdict to judge that the joint intelligence committee machinery, which I have known well and respected, was corrupted in a way which will leave damage for decades to come . . . It is impossible to believe that Sir Anthony Duff, Sir Percy Cradock or Dame Pauline Neville Jones, to name but three heads of the JIC with whom I have worked, would ever have conducted themselves as John Scarlett did with Jonathan Powell and Alastair Campbell over amending the statement on Iraqi weapons of mass destruction.' Lord Owen, 'The Ever Growing Dominance of No. 10 in British Diplomacy since 5 April 1982', Lecture at the London School of Economics and Political Science on 8 Oct. 2003, available at URL <http://www.lse.ac.uk/collections/LSEPublicLecturesAndEvents/events/2003/20030915t1227z001.htm>.

nal policy, but for the confidence held by internal constituencies in the correctness of the government's judgement. (The impact of any proven bias in British intelligence assessments on Iraq would hardly be helpful, for instance, in rallying the UK's own moderate Islamic community to support the anti-terrorism effort.) In the UK, the JIC's analytical skills have also been an important bulwark of the British–US intelligence relationship, given that the amount of 'raw' intelligence that British agencies can contribute to the partnership is relatively small. Just as the USA became reluctant to share intelligence with the UK after a series of British double agents working for the Soviet Union were exposed in the 1950s and 1960s, the fact that US intelligence has been exposed to its own share of criticisms after 11 September 2001will not necessarily prevent it from raising questions about British judgement and reliability.

Bring in the private sector?

When the state is seen to be failing in the provision of an important service, it is often natural to turn to the private sector for help. Either there is something inherently inefficient about the current system—in which case it should be adapted and changed—or the whole enterprise is so inherently difficult that it needs to draw on the widest possible pool of talent and experience. On either view, there could be merit in turning to the private security sector and exploring the possible contributions of business more widely. Private experts could contribute both analytical and human intelligence resources from areas which the official system does not reach. They are more likely to provide 'out of the box' thinking, informed by the foresight and nimbleness characteristic of private risk assessment at its best. More generally, opening up the assessment process to new actors representing an important part of British society ought to serve the same aims of balance and comprehensiveness which the JIC's original creators had in mind. Putting intelligence in touch with the British public and *vice versa* is not in itself an ignoble aim, any more than the idea of publishing intelligence-based 'dossiers' on important security issues of the moment is wrong per se. The nub of the issue is how to make sure that the information is as credible as it is accessible.

Specifically, one could consider opening up the process of recruitment to the Cabinet Office Assessments Staff, which actually drafts the papers for the JIC. The organization already recruits through open competition from all those holding the appropriate rank in government service. It would be simple to expand its catchment area. If large British companies, or private firms or academic institutions engaged in the business of intelligence analysis, were allowed to second talented individuals for two-year postings to the Cabinet Office, a considerable body of intelligence expertise and experience of Whitehall could be built up over time within the private sector. Those who proved their worth in both fields could eventually be qualified to hold more senior posts within the central intelligence structure. It is no secret that some of the best and brightest British graduates become analysts of one sort or another in the City of London, where the essence of their work is to act on imperfect data and to try to look into the future, in order to make money. Why not bring their skills to bear on more important matters?

The benefits that could be gained from private-sector involvement are not limited to analytical skills. One of the effects of globalization has been the creation of companies with a literally worldwide reach, allied with a truly global culture. Their senior employees are no longer drawn exclusively from the 'motherland' but from a range of different regions and cultural backgrounds. Often, the only collective culture to which they owe true loyalty is that of the firm in which they work. At the grass-roots operational level, meanwhile, these companies extend their tentacles into nearly every corner of the world, making their employees—both local and expatriate—uniquely well placed to assess local moods, attitudes and politics.

The best collection principle for human intelligence is to make use of everyone, or at least everyone who is on your side. This notion lies behind the best designed anti-criminal and anti-terrorist information campaigns. In such cases the authorities believe that members of the public, alert and properly briefed, have a much greater chance—if only because of their numbers—of picking up indications of a criminal enterprise or terrorist attack than do the official organs themselves. The same argument can be made for the added value to be gained from private intelligence collection. Private firms are more numerous and very often have greater cultural penetration than formally structured intelligence services. Senior officials of important global firms invariably hold high social positions in the community and cultural life of the cities in which they are stationed and, in capital cities especially, are likely to be well integrated into the business and government elite. They are thus ideally placed to gather intelligence: if only a way can be found to enlist and make use of their efforts that does not conflict with their own principles, and with the prime commercial purpose of their activity.

V. Conclusions

Other contributions to this volume focus on the business sector's own vulnerabilities and the options for its protection.[16] This chapter draws attention, rather, to the long-standing traditions of public-sector dependence on private-sector expertise and assistance, which can apply as much in the security field as in any other.

The events of September 2001 and their aftermath have exposed at several points the difficulty faced by traditional state security policies and intelligence systems in adjusting to the reality of an age when whole societies, not just national borders, are under attack. Universal vulnerability makes the accuracy

[16] See in particular chapter 15 in this volume.

of intelligence a universal concern, yet the latest attempts by intelligence specialists and their political masters to reach out to the public have been a mixed success at best. The private sector has not precisely been excluded from the picture, but in public perception has often provided added reason for confusion and concern—*vide*, for example, the conspiracy theories that business interests were behind the choice of Iraq as a target in 2003 and/or that they have profited improperly from the aftermath of the war.

Drawing private-sector expertise, including that of professional security companies, more systematically into the business of threat identification and assessment as well as into the provision of remedies is certainly no panacea. If successfully done, however, it could bring a double benefit. Not only would private experts be likely to bring a genuine accretion of information, analytical skill and new policy thinking, but the establishment of an open and systematic partnership between them and the state authorities could also be an important victory for transparency and a step towards the restoration of public trust.