The Politics of Warning: Terrorism and Risk Communication

LAWRENCE FREEDMAN

The problem of risk communication in the context of imperfect intelligence regarding a prospective, rather than actual, terrorist attack is examined in order to assess recommendations for precise guidance for the public. Particular problems are noted with the iterative quality of risk communications about terrorism, as they allow the terrorists to change their behaviour, the difficulty of offering tactical warning without a prior strategic analysis, and the tendency to focus on the vulnerabilities of a society rather than the intent of the terrorists. These issues are assessed through a case study of the Bali attacks of 2002, before an analysis of the American experience following the attacks of 9/11. This experience confirms the difficulties of attempting to convey risks to the public by altering public alert levels.

The question of how governments should prepare their publics for possible terrorist attacks has been to the fore ever since 11 September 2001. The intelligence material on the threat is bound to be incomplete and uncertain: otherwise there would be no issue as attacks could be prevented without spreading any anxiety that they might not. Imperfect intelligence results in imperfect messages to the public with all the associated problems of credibility. Governments that say nothing when aware of a possible threat will be accused, should one materialize, of failing in their duty. Governments which warn regularly, but without much happening, will be accused of alarmism. If they warn, but can offer no useful advice, then the public will have another reason for dissatisfaction. Unless high risk areas can be identified with some specificity then it is unclear what can be achieved through general exhortations to be vigilant and take reasonable precautions in everyday activities. The sins of omission or commission compete, with bad advice generating panic at one extreme and apathy at one at the other.
After each terrorist incident there is a clamour for better advice. The UK Parliamentary Intelligence and Security Commission, for example, complained after the October 2002 Bali bombing that FCO Travel Advice was ‘not well formatted’, too complex and confusing, combining elements of reassurance with routine language recycled from edition to edition. The demand was for the terrorist threat to British citizens to be more clearly identified, and the ‘sensible precautions that could be taken by them clearly described’. This is a normal demand. The US General Accounting Office recommended that public warning systems on threats to homeland security should include ‘specific, consistent, accurate, and clear information at the threat at hand, including the nature of the threat, location, and threat time frames’. In addition guidance should be included on ‘actions to be taken in response to the threat’. The study warned that if the threat information is inadequate, the public might ignore the threat or engage in inappropriate actions, some of which may compromise rather than promote the public’s safety.1

Such demands, however, based on a model in which high-quality intelligence information is inputted to provide an output of reliable risk communication are unrealistic. This article examines the problem of risk communication in the context of imperfect intelligence regarding a prospective, rather than actual, terrorist attack, which may or may not occur. My particular focus is on the American experience following the attacks of 9/11, although some consideration is also given to the British. Before this analysis, I provide a framework for the consideration of warning and risk. This leads to proposals for discussions of threat assessments at the levels of generality that the available evidence can sustain, rather than attempts to measure and grade threat levels.

INTELLIGENCE AND THREATS

The most important work on risk communication and terrorism has concentrated on post-attack responses. The July bombings in London, for example, demonstrated the importance of reliable information during a fast-moving situation. A chemical and biological incident, which would have a developing impact over time, would make even greater demands on official systems of risk communication in order to get trusted advice to potential victims.2 The credibility of these systems, both before and after major incidents, will depend on past levels of transparency and how previous incidents have been managed, especially if things have gone badly wrong.3

There are, however, distinctive problems when attempting to communicate prospective risks. Baruch Fischhoff has argued that a high-quality model of the threat will encourage ‘consistent alarm standards’. If these are properly
understood then citizens will ‘understand why false alarms are inevitable and minimize their costs—including cumulative apathy’. To develop such an understanding he proposes linking public opinion with public policy, in a structured discussion of how best to respond to the challenge. In a national survey designed for this purpose he found strong support among Americans for ‘honest and accurate information about terror-related situations, even if that information worries them’. In a similar vein, the Partnership for Public Warnings in the US makes a formidable case for those with potentially alarming information to take the public into their confidence and not be deterred by concerns of either generating panic or being accused of ‘crying wolf’.

There are two basic problems with such a requirement. First, because the available information is normally poor, the consequential threat assessments are often speculative. Second the communications will be reflexive. A warning that a hurricane is imminent would be an example of a non-reflexive communication: the developing weather system is not influenced by what is being said about it. A warning of an imminent terrorist attack is reflexive: the communication allows the terrorists to change the threat they pose. This is a particular problem of strategic risk communications. Strategy involves inter-dependent decision-making, so that a decision by A must anticipate the decisions of B and how they might be influenced by A’s own future behaviour. If this process is transparent, because A must share its risk assessments with the public, or just makes conspicuous provisions in response, then B will receive valuable intelligence and alter his behaviour accordingly to confuse and surprise A. So because strategic risk assessments anticipate decisions that others have yet to make they are bound to be imperfect.

The problems A faces in understanding the developing intentions and capabilities of B is hardly an unusual problem for intelligence agencies. They are aggravated in the case of terrorism. The military capabilities and political intentions of states provide clear targets for intelligence collection and the range of their strategic options can be delineated. Sub-state groups, operating covertly at all times, are much harder to track and their attack options are numerous. Intelligence collection will be hampered by the fact that only a small number of militants will be involved and they will aim to merge with the civilian population or look for sanctuaries across borders.

Intelligence agencies have to cope with large amounts of clutter and background ‘noise’, sometimes planted in a deliberate effort to confuse them, from which they have to pick out relevant material. At the time of 9/11, the FBI’s counter-terrorism division had some 68,000 outstanding and unassigned leads dating back to 1995. There are guides for how to find the vital nuggets: look to sources that have been dependable in the past, or
demand that there is corroboration from multiple sources and a fit with pieces of otherwise unrelated information. These guides may be of limited value when the ratio of reliable information to hearsay, rumour and hoax is extremely discouraging. Furthermore, keeping track of such groups, operating on the intersection between domestic and foreign intelligence agencies and across jurisdictions, requires high levels of cooperation. This is hard to achieve in even quite undemanding circumstances because of the legal impediments to intelligence sharing between countries and the institutional impediments to sharing within. It has been said that only the intercession of senior leadership and ‘brute force’ ensures sharing between the CIA and the FBI. Domestic agencies may have to choose between gathering information on the same group to gain prosecutions in domestic courts or finding out more about the group’s organization and plans (the ‘string ‘em up’ or ‘string ‘em along’ problem). Other countries and agencies may not be trusted to look after sensitive information, or perhaps particular nuggets might be held back until they can be traded for something equivalent in return.

For purposes of public safety, governments wish to be able to issue warnings of imminent attack. To alert those who might be able to prevent the attack or warn those that might be vulnerable something must be said about method, targets, timing and location. It is not impossible that intelligence agencies might come across material that provides just this sort of information. Alternatively, law enforcement personnel may stumble across the actual preparations for an attack. It is quite rare, however, for such information to arise out of the normal course of the assessments process. Former CIA analyst Jack Davis argues that there are inherent limits to what can be achieved in the area of what he calls tactical warning analysis. This he describes as being characterized by

a search for and evaluation of diagnostic information about incident, perpetrator, target, timing, and modalities. The goal is to deter and limit damage by identifying in advance when, where, and how a declared or potential adversary will forcefully strike the United States directly, mount a challenge to US forces, personnel, or interests abroad, or make a menacing weapons breakthrough.

He contrasts this with strategic warning analysis. This aims for analytic perception and effective communication to policy officials of important changes in the character or level of security threats that require re-evaluation of US readiness to deter, avert, or limit damage—well in advance of incident-specific indicators. Thus
strategic warning is characterized by inferential evidence and general depiction of the danger.

This fits with my earlier definition of a strategic risk communication, in that the analysis must be pitched at a level that makes it possible to form a view and so anticipate the adversary’s strategy. Although public warnings are based on tactical analysis, Davies points out that not only are they the most difficult to provide but they become even harder if the underlying strategic analysis is inadequate. This is why he would make this the priority because it orients policy-makers to the broad nature of the threat and provides a basis for allocating resources to prepare for specific attacks.

A strategic warning analysis must involve a conceptual framework through which to evaluate new information about the future development of the adversary’s strategy and convey the sort of problems that may result. This will take what may be meagre, muddled or vague information and make sense of it by drawing on some crucial context or linking material. The analysis cannot proceed without such a framework, yet frameworks based on poor information risk being poor themselves. The poverty may become circular as frameworks are reinforced by information that appears credible simply because it fits with a core hypothesis.

This is not the only sort of difficulty facing attempts to generate serviceable strategic analyses. Precisely because they may well influence resource allocation they are politically loaded. Davis notes that even with high-quality assessments there are still problems of getting policy-makers to commit to a particular description of the threat, because defining a problem in a particular way has bureaucratic and political consequences. There is likely to be a direct relationship between the uncertainty of the analysis and the role of these other influences. He notes, for example, that while 9/11 was presented as a failure of tactical analysis it was also a failure of the strategic. This was less because responsible agencies and individuals were not warning of the danger posed by al-Qaeda, or that protective measures had not been urged, but because they were not taken seriously enough. Davis cites this as an example of ‘inconvenient warning’. This is one that requires policy-makers to ‘pay the political and economic costs of direct expenditures, inconvenience, disapproving special interests, and breaking of bureaucratic rice bowls’. The immediate costs of committing to this threat outweighed the potential costs of failing to commit.

This reflects the purist view of a professional, concerned that the integrity and value of an assessment is being undermined as a result of inappropriate, extraneous influences. The problem, however, goes beyond the reluctance of particular politicians, bureaucrats or officers to treat assessments with the objectivity and respect those who produce them believe they deserve.
A distinction here can be drawn between an *intelligence estimate* and a *threat assessment*, though they may be both concerned with the same terrorist adversary and the terms are often used interchangeably. An *intelligence estimate* for A offers guidance on B’s future attitudes and behaviour, attempting to second-guess the decisions of B’s leaders and appreciate the factors which shape its decisions. Because it must anticipate decisions that B’s leaders have yet to take, a firm prediction can never be offered but only a range of possibilities. A *threat assessment* interrogates intelligence estimates in the light of the perceived vulnerabilities of A. B’s growing strength may be irrelevant if it cannot be turned into a source of real harm, while some modest capability may turn out to be significant if it can be directed at some critical weakness of A. With a threat assessment the main question is likely to be ‘what might B do which might expose A’s vulnerabilities?’ rather than ‘what is B most likely to do?’ It thus requires an analysis of A’s vulnerabilities, and these can be matters of heated domestic controversy, turning on the relative importance of economic health, social cohesion, political philosophy, energy dependence, international prestige, military strength, or any combination of these.

It would be neat if we could say that intelligence estimates are produced by intelligence agencies and become threat assessments at the point where they mix with the wider concerns of policy, but it is very difficult for the intelligence professionals to isolate themselves from the concerns of policy, even when producing their estimates. Because they act in anticipation of the other, A’s intelligence agencies must form a view of B’s likely responses to A’s own actions. It is often a complaint of intelligence professionals that they are kept in the dark about policy options. For their part, policy-makers may complain that an estimate which notes how a particular course of action (say war against Iraq) might appear provocative to the adversary and lead to an unwelcome response, serves as a commentary on the wisdom of government strategy. Policy-makers may also take it for granted that the potential adversary has the same perception of national vulnerabilities as they do and may be disinclined to trust estimates that suggest a quite different perception. More seriously, an estimate which suggests that an adversary is unlikely to develop a particular capability can come as a blow to those with a stake in the development of the counter-capability.

It is not necessarily the case, therefore, that intelligence estimates inform threat assessments which then in turn inform strategic choices. This may seem to be a logical way to proceed, but influence can move in the other direction as advocates of particular strategic choices develop theories of vulnerability to rationalize their preferences and then seek intelligence estimates which add weight to their theories. Certainly, much debate on terrorist threats starts with a locally-generated sense of vulnerability as much as an externally-generated intention to attack. John Mueller has written of the
factors which encourage exaggeration of the threat and how after 9/11 attempts to convey how limited the risks posed by terrorism really were got crowded out by alarmist statements about the threat to the whole American way of life.\textsuperscript{10}

It may well be that when the intelligence model of B is vague and poorly developed, threat assessments may be influenced largely by models of A’s vulnerability. Some evidence for this possibility is found in an evaluation of the performance of the US intelligence community in combating terrorism which drew attention to the vast improvements in ‘vulnerability assessments across the different elements of society (including in particular in the area of critical infrastructure)’.\textsuperscript{11} Frank Furedi has argued that approaching the terrorist threat from ‘the standpoint of vulnerability encourages an attitude of pessimism, dread and foreboding’. This is because perceptions of vulnerability have a ‘free-floating character that attach themselves to a wide variety of phenomena’, encouraging explorations of speculative risk.\textsuperscript{12}

One example of this is ‘cyberterrorism’. This was a response to the growing importance and impact of information technologies during the 1990s, which suggested that terrorists could achieve their aims by preying on advanced societies’ growing dependence on these technologies. This literature developed with little evidence of any actual terrorist interest in such attacks (although considerable evidence of criminal interest). Even after 9/11 there were warnings of how al-Qaeda might be tempted by such methods. US Homeland Security Director Tom Ridge warned in April 2002 of the ‘worldwide havoc’ that could be created by sitting at a computer. Explosives were not necessary ‘to cripple a sector of the economy, or shut down a power grid’. The concerns about a ‘digital Pearl Harbor’ consistently exaggerated the ease with which ‘cyber-attacks’ could be made and the severity of the consequences.\textsuperscript{13} After 9/11, there was a natural interest in scenarios involving the maximum violence and the greatest number of fatalities. This produced a link with weapons of mass destruction, which was part of the underlying rationale for the Iraq War.\textsuperscript{14} In 2004, the most important contribution to this debate came with a book on ‘nuclear terrorism’.\textsuperscript{15} Undoubtedly this represents the worst that could happen, and, as the book demonstrated, it is not a possibility that can be safely ignored. In no sense, however, did this represent the most probable type of incident. If the question was asked what terrorists are most likely to do then far more modest and manageable answers emerge. Past practice would suggest, for example, that the most likely single target of terrorist attacks is a McDonald’s restaurant, although in only a few cases have casualties been involved. If every time there was a heightened alert Americans worldwide were urged to avoid McDonald’s this would seem an odd response – economically damaging to McDonald’s while saving few lives. Meanwhile, in public policy terms the nuclear threat requires urgent attention,
but in public information terms it does not, for it remains unlikely and there is not a lot that individuals could do should it occur.

I have argued so far that leaving aside good luck effective tactical warning is most likely to result from a high-quality strategic analysis. This is difficult to produce out of poor information on B’s intentions and capabilities, so when constructing threat assessments some reliance will be placed on what is understood about A’s vulnerabilities. As individuals and institutions have an interest in particular threat assessments, they may well seek to influence the form they take. This can produce analyses which emphasize contingencies that resonate within A although they may be of scant interest to B.

What then happens when this threat assessment is turned into a risk communication? Here further distortions occur because of the wider purposes of risk communications. The act of communication transfers responsibility for dealing with the risk. If travellers have been told that a particular country is unsafe they cannot complain should they find themselves caught up in something unpleasant. If financial institutions have been told that they are likely to be targeted they cannot complain if their business continuity is inadequate. For governments there are obvious advantages in transferring responsibility in this way. For the recipients the communication may be less welcome. They may be grateful for the warning and prepared to accept a degree of responsibility for acting upon it, especially if the communication is private. Even then it may be difficult to identify appropriate responses geared to the probability and severity of the threat. Extra costs, in the form of more security guards, might be tolerable: shutting down whole businesses, evacuating public spaces or grounding airlines might be less so. More problems may result if the communication is overt and public, for then others will take note. To be put officially ‘at risk’, in some way ‘unsafe’, can be a form of stigmatization. Financial institutions, for example, will warn of the economic impact, including increased insurance costs, of a loss of confidence in a particular location—the City of London or Wall Street. Another example would be air travel, which is affected by popular views of its safety. Airlines suffer when the risk of flying becomes too high. If tourist destinations are labelled as hazardous, even if there has been no attack, then they will be put at financial risk. They may therefore resent foreign governments issuing alarming and, they would consider, exaggerated warnings.

The difficulties in communicating risk of a possible attack become particularly severe with members of the public because of the lack of useful advice on how to reduce this risk or mitigate its effects. There are limits to what individuals can do to protect themselves when the degree of personal danger they face is in practice hard to calculate and may well be very small. By and large governments do not want the general population to panic, or avoid city centres or air travel, or disrupt their normal patterns of life in any
way. It is still, however, assumed that if there is information of an imminent attack then it should be shared.

There is therefore pressure on governments to consider the impact of warnings on the recipients. While it may suit their purposes to transfer responsibility for limiting the potential damage of a terrorist incident, in the process they may generate a requirement for secondary forms of damage limitation. Thus in contrast to a warning process that may start with excellent information which leads to a threat assessment which in turn leads to a risk communication, this discussion suggests the possibility of a reverse process by which, in situations in which the information is poor, the desire to avoid certain forms of risk communication, with their adverse consequences, and pressure to divert resources to meet politically significant vulnerabilities, may exercise a greater influence on the content of threat assessments.

Strategic risk communication is not therefore simply a question of finding the right language to pass on intelligence information about possible attacks. The inherent uncertainty in the information, the ability of the attackers to adjust their behaviour on the basis of what the defenders have revealed about their state of preparedness, and the fact that warnings have political, economic and social effects even when no attack materializes, must affect the calculations which lead to warning events. Because they are politically loaded and involve the transfer of risk, non-governmental organizations, or even other governments, have an interest in influencing the content of official risk communications, and different agencies of government may differ amongst themselves about where the risks lie. Officials do not always speak with one voice and official communications are not the only ones available to the public.\textsuperscript{16}

Government assessments will be subjected to critical analysis through the media, with pundits and politicians all having their say. Think-tanks and academics may issue warnings of their own, based on their analyses of the behaviour of terrorist groups, or challenge the warnings given by government. After the Bali bomb, for example, the authoritative Australian Strategic Policy Institute issued its own assessment, rating ‘the risk of terrorist attack on Australia, and on Australians overseas as high . . . more likely than not’.\textsuperscript{17} Just after the July 2005 London bombings a paper produced under the auspices of Royal Institute of International Affairs was widely quoted in the press for apparently supporting the views of those who argued that Britain had put itself at unnecessary risk as a resulting of supporting a reckless American foreign policy.\textsuperscript{18} Alternatively, there may be charge that alerts are being used for political purposes, perhaps to distract attention from other news, or alternatively that a real peril is being played down because dealing with it risks offending a foreign government or creating the equivalent of a state of emergency. In open societies government
provides one voice among many, competing for attention with ‘risk entrepreneurs’ with their own distinctive angles on the dangers ahead. As Furedi demonstrates, once it is accepted that any vulnerability can be translated into a terrorist opportunity, then there are incentives for special interest groups to use the terrorist theme to pursue their own agendas, including a major change in foreign policy, resulting in a steady stream of scare stories.19

TERRORISTS AS RISK ENTREPRENEURS

Lastly, there are the terrorists themselves. By issuing a warning governments are also transferring risks to them. These may lead them to assume that the authorities are aware of their activities and so they are more likely to be caught if they press ahead with an attack. By then deciding not to act terrorists can reduce the credibility of future warnings. Alternatively, through hoaxes or their own messages they can confuse or undermine the official system of warnings, maximizing disruption and making it easier to mount surprise attacks. In such ways terrorists are the ultimate risk entrepreneurs. They may warn of future attacks, perhaps with a hint of type of target or location in order to maximize the impact on public perceptions. Most seriously they may actually mount a successful attack. This is the most effective risk communication of all, because it adds reality to all types of warnings and will make itself felt in individual and collective risk communications. It will be assumed that if the terrorists are capable of one major attack they will be capable of another and that this must influence individual calculations of risk. Over time the absence of further attacks will reduce the level of concern and also the degree of risk aversion.20 Among New Yorkers, for example, in late 2001, risk aversion was reflected in around 25 per cent delaying or cancelling plans to travel by air and around 18 per cent deciding to drive into Manhattan less often or use its mass transportation system.21 These affects declined only gradually. The impact on air travel was particularly dramatic, and was worldwide in its impact. Similar, but more modest effects were noted after the anthrax attacks of October 2001, which were largely related to handling of mail. This behaviour was at its most pronounced while there was still concern that contaminated mail might be circulating around the US postal system.22

Different types of terrorism raise different issues of warning. As a contrast to the challenge posed by contemporary Islamist terrorism consider the Provisional IRA’s campaign in mainland Britain up to the 1998 cease-fire. From the 1970s to the 1990s Londoners became familiar with a terrorist threat. The campaign took varied and unexpected turns over many years, but it had certain features that over time came to be well understood. Those most
in danger were politicians and military personnel as they might be attacked without warning. The ordinary public could expect to be inconvenienced but they would be unlucky to be hurt or maimed themselves, although of course some were. For their own protection there were certain rules to follow: not leaving bags unattended, checking under cars and looking for wires protruding out of packages. The best advice, however, was to do what the police asked. There were many false alarms but there were sufficient real explosions to know to stay clear of particular places when told do so. This was possible because, by and large, with some terrible exceptions, there were timely warnings. These came from the terrorists themselves.

These warnings were given through coded messages, usually one hour before the timed explosion. To gain credibility these messages were often correct. For the IRA they had a number of advantages: they could demonstrate that this campaign was directed against physical targets or the military and politicians but not ordinary civilians. They could also maintain some control over the process. If things went wrong the security services could be blamed for not acting quickly enough or for evacuating people from the wrong location and even in the wrong direction. Warnings were another weapon in the armoury. They could be used to add to the disruption, by being either non-specific (a railway station will be attacked) or simply mischievous (warnings were given but nothing was found). There was therefore a useful way in which the IRA could get ‘two bangs for their buck’ by following actual attacks with hoaxes.

So in this case warnings served the terrorists’ strategy. In a campaign designed to cause disruption over an extended period, a series of small incidents, reinforced by hoaxes, could do as much as a single big hit. While at times the actions of the IRA were curious, at the peak of their campaigning they were understood well enough for the emergency services and the public to adjust to them, and they could be used to reinforce tactical objectives. There was a long learning process as the patterns of behaviour and the references began to be appreciated, not only by the security services but, in a cruder form, by the public. That is to say that there was a reasonably reliable strategic threat analysis and usually, but not always, with the IRA’s connivance, sufficient information for tactical warning. The engagement was sufficiently well understood for governments to avoid charges of either paranoia or complacency.

The sort of terrorism associated with al-Qaeda is quite different. It operates on a global rather than local scale and has shown no interest in using terror as a bargaining counter. It has sought mass casualties. There is a question about whether this actually reflects a strategy. It may be that death and destruction can be sought for their own sake, as acts of cleansing or retribution, but without a political purpose. Then the problem is not one of terrorism but
pathological violence. If it is a strategy, this terrorism can be assumed to have
the objective of causing psychological effects (terror) that in turn cause
political effects. The aim is to put the target political system under
severe strain leading to fundamental changes in policy. In order to maximize
civilian casualties, then, surprise is essential. To achieve this, terrorists can
benefit from a wide range of choices with regard to target, weapons and
location. Partly because of this incidents are few and geographically
dispersed. The warnings issued by al-Qaeda and associates have normally
been expressed in lurid terms but only vague detail. In particular countries
they are directed to persuading foreigners to leave; elsewhere they may be
presented as part of a claim to persuade Western governments (‘the
crusaders’) to change their ways and leave the Moslem world alone.

Since 9/11 al-Qaeda (which is best understood as an umbrella term for a
variety of groups, linked ideologically and sometimes organizationally) has
changed. It is no longer centrally directed with a base in Afghanistan. Instead a
number of groups acting with the same philosophical underpinnings have been
acting more or less independently, often pursuing distinct national agendas as
well as more global causes. Specific campaigns continue, with substantial
popular support, in Chechnya, Kashmir, Pakistan, and now Saudi Arabia and
Iraq. At the same time the conflicts in Afghanistan, Palestine and Iraq have
served as rallying calls for militants and provide a focal point for action.

For those trying to predict the next terrorist outrage there is not much to go
on. The sheer range of possibilities adds to the challenge for the intelligence
agencies. The British Foreign Secretary noted that after 9/11 the volume of
incoming intelligence had increased ‘by a factor of at least ten’, and that in
the period leading up to the October 2002 Bali bomb at least 150 separate
reports covering at least 20 different countries were received. An al-Qaeda
broadcast on al-Jazeera may provide a sign that something is up, but exactly
where the attack may come may not be clear. The organizers of these groups
have shown increasing sophistication in attacking what they consider to be
Western vulnerabilities. This is reflected in attacks designed to undermine the
Saudi economy by targeting expatriates or the careful assessment that led to
an appreciation of the potential for disrupting the international coalition
supporting the Iraq War by attacking Madrid just before the Spanish
election.23 In his pronouncements Osama bin Laden has been offering
increasingly subtle political and economic analyses of the impact of his
group. On 15 April 2004, for example, he offered a ‘truce to them [Europe]
with a commitment to stop operations against any state which vows to stop
attacking Muslims or interfere in their affairs, including [participating] in the
American conspiracy’. In a message to the American people just before the
2004 presidential elections he drew attention to the economic effects of 9/11
(see http://news.bbc.co.uk/1/hi/world/middle_east/3627775.htm).
The comparison of the IRA with al-Qaeda indicates that different types of terrorist groups have different approaches to warning and that these may evolve over time. It could be said that the IRA assumed that it did not need to influence its enemy’s strategic threat analysis but saw value in influencing its tactical warning to produce maximum confusion and disruption. Al-Qaeda has shown little interest in influencing tactical warning but a growing interest in influencing strategic analyses.

**BALI**

These various aspects of the problem can be illustrated by looking at the case of the attacks on the Indonesian tourist resort of Bali on 12 October 2002. That night a number of explosive devices were detonated. One exploded outside a packed nightclub and some 200 people from 20 countries were killed, including 88 Australians and 26 Britons. In both Australia and the UK victims and their relatives expressed anger and a conviction that they had been let down, especially after evidence emerged that Americans appeared to have been given better guidance. If they had also known about the dangers, they claimed, they would have avoided Bali. This led in both countries to parliamentary inquiries. The case illustrates the complex interaction between developing intelligence, strategic threat assessments and tactical warning.

The established US State Department travel advisories concerning Indonesia, issued in September and November 2001, urged US citizens to defer non-essential travel. This was largely because of separatist violence and ethnic strife in a number of provinces and communal tensions in West Timor. Only in the border areas were terrorist groups mentioned—militants in Central Java that had threatened to ‘sweep’ Americans from Indonesia and the Abu Sayyaf group, which had kidnapped American citizens in the extreme southwest Philippines, near Indonesia. The advisory concluded with a non-specific warning reflecting ‘information that extremist elements may be planning to target U.S. interests in Indonesia, particularly U.S. Government facilities, but also possibly including commercial and other private targets’ (US State Department, 25 September 2001 and 25 November 2001). There had been a series of 24 attacks against churches and leisure venues in Indonesia on Christmas night 2000.

Of the extremist groups then operating in Indonesia, the most significant was Jemaah Islamiyah (JI), which promoted the idea of an Islamic state in Indonesia and elsewhere in Southeast Asia. It was believed to have developed links with al-Qaeda, and received money, explosives and operatives for terrorist activities. Hard information on planning for attacks was found in November 2001, when computer files and documents found in an al-Qaeda house in Afghanistan revealed the travels and contacts of Ayman al-Zawahiri,
Osama Bin Laden’s number two. This led to the Singapore authorities arresting 13 Muslim men who were alleged to have plotted mass slaughter by truck bombs at key locations including the Australian embassy, and who also had links to JI.\(^{25}\) Despite Singapore’s demands that it curb JI, Indonesia responded cautiously but on 9 January 2002 an Egyptian al-Qaeda suspect was arrested. Meanwhile a number of Indonesians with JI links were arrested in the Philippines. In June 2002 an al-Qaeda operative, Omar al-Faruq, a Kuwaiti, who had been working with JI since 1998, was arrested in Java and turned over to the United States. Under CIA interrogation in early September he admitted that he was planning attacks against Western interests in East Asian countries, supported logistically by JI. When apprehended he was believed to be planning an attack on the US embassy in Jakarta.\(^{26}\) Intelligence from this source, combined with intercepted communications involving JI, indicated a potential strike against ‘a Western tourist site’. An unpublished CIA alert in late September listed Bali as a possible target although central Java was considered most likely.\(^{27}\) The assumption was that such an attack would be reactive, following the possible arrest of certain individuals (presumably JI activists). As no arrests had been made the exact status of the threat was unclear.

On 6 October 2002 al-Jazeera broadcast a two-minute tape allegedly containing Osama bin Laden’s voice, threatening a strike ‘against US economic interests’ if Washington did not halt attacks on Arab and Muslim countries. The next day al-Zawahiri called on Muslims to launch attacks on ‘the criminal gang at the White House’. While US officials suggested there was no need to raise the existing security level, already reasonably high,\(^{28}\) it was possible that this was taken as a signal by al-Qaeda supporters and affiliates, including JI, to begin a new round of attacks. Certainly it was followed by an upsurge in violence: the shooting of a US Army Special Forces soldier in the Philippines on 2 October, an attack on a French oil tanker near Yemen on 6 October and the death of a marine shot by two gunmen in Kuwait two days later. In late October a US diplomat was shot dead in Amman.

Having previously focused on communal violence as the major risk to US nationals in Indonesia, the Jakarta embassy on 9 September advised of the risk of a ‘credible’ terrorist attack. A further caution of 20 September mentioned the Yogyakarta region, 200 miles from Bali. The major concern, however, was the threat to diplomatic targets. As a result the US embassy was closed for six days in September. This analysis of the threat was reinforced by a grenade attack on an unoccupied embassy residence in Jakarta on 23 September. This prompted consideration of a draw-down of diplomatic personnel.\(^{29}\) The embassy did recognize that not only diplomats were at risk. On 26 September 2002 it issued an ‘embassy notice’ that stated: ‘Americans
and Westerners should avoid large gatherings, and locations known to cater primarily to a Western clientele such as certain bars, restaurants and tourist areas.’ This warning was not reflected in the State Department’s advice for Americans travelling abroad.\textsuperscript{30} In addition, neither in their travel advice nor in their embassy notices did the US make any reference at all to Bali. Following the al-Qaeda tapes appearing on Al-Jazeera, a new worldwide caution was issued by the State Department on 10 October, only two days before the attack in Bali. It contained no reference to Bali, Indonesia or even Southeast Asia. A classified warning circulated that same day was no different. An American citizen paying close attention to travel advice would have been aware of growing concern about terrorism, but would have assumed that diplomatic targets were more at risk than tourist targets, and that Bali was not particularly at risk.

Australian advice followed a similar progression. Although the availability of ‘a range of soft and symbolic targets for anti-Western Islamic terrorists’ in Southeast Asia was noted in January 2002 by Defence Intelligence, incidental violence arising from local conflicts was still seen to pose the greatest threat to Westerners in Indonesia.\textsuperscript{31} As in the US analyses, the threats mentioned in the CIA material were contingent upon arrests that had not occurred and ‘official’ targets, such as embassies or military personnel and units, were deemed to be most at risk. Faruq’s arrest in mid-2002 prompted increased internal debate about possible terrorist attacks against Western interests in Indonesia, and whether there might be a significant move away from ‘relatively small events directed at domestic targets’. On 20 September the Australian Department of Foreign Affairs and Trade issued travel advice for Indonesia that specifically referred to the general threat of bombing by terrorists, and on 3 October the embassy in Jakarta issued an embassy bulletin, equivalent to the American embassy notice, referring to the possibility that militant groups might engage in ‘intimidatory activity against night clubs, bars and other places where expatriates are known to gather’ around religious holidays.\textsuperscript{32} Then, following the US caution of 10 October, the DFAT travel bulletin stated that: ‘In light of the warnings by the United States Government, Australian travellers and residents overseas are advised to remain alert to their own security.’

In Britain the Joint Intelligence Committee (JIC) produced a paper in May 2002 on International Terrorism in South East Asia, noting the al-Qaeda presence in Indonesia and the links with JI, and that the Indonesian authorities had not placed a high priority on dealing with terrorism. The main threat to British interests in Indonesia, assessed as HIGH (threat level 2), was to diplomatic premises, though the reports on the possibility of wider attacks and the mention of tourist sites in Indonesia, including Bali and nightclubs in Jakarta, were noted. The FCO travel advice for Indonesia issued on 27
August 2002 described most visits to Indonesia as ‘trouble free’ but suggested care when visiting some regions and that others should be avoided altogether. Bali was not listed. There was a general observation about the ‘heightened terrorist threat to US and UK interests worldwide’, with Indonesia one country where there was ‘an increased threat’ requiring ‘extra vigilance’ in public places. As for Bali, the main advice was to watch out for crime. The British embassy in Jakarta closed down for two days during the anniversary of 9/11. The failed grenade attack on an American diplomatic residence in Jakarta on 23 September, however, tended to confirm that diplomatic premises were most at risk. The Parliamentary Intelligence and Security Committee (ISC) acknowledged that there was no ‘intelligence that described or directly related to any form of terrorist attack on Bali on or around 12 October’, and so there was ‘no action that the UK or its allies could have taken to prevent the attacks’. After the 23 September attack it took two weeks (to 9 October) for the Security Service to issue an internal report on Indonesia. The ISC identified a ‘serious misjudgement’ by the Service in not upgrading its assessment of the threat to British interests from ‘significant’ to ‘high’, given the new intelligence and the ‘reluctance of the Indonesian authorities to deal with terrorism’. The problem therefore lay in the intelligence assessment rather than the travel advice, which was ‘proportional’ to the threat assessment. At the same time subscribers to an e-mail service in Indonesia were encouraged, on 27 September, ‘to be more circumspect than usual, especially in the evenings’. On 3 October they were also warned of the unpopularity of bars and night-clubs with Islamic activists. British Foreign Secretary Jack Straw later remarked that ‘There were generic threats, but there was no information that could have enabled us to warn in advance of this atrocity’. As with the Australians, the British drew attention to the fact that the Americans, despite circulating the alert and issuing a notice from the Jakarta embassy, had not specifically warned their nationals not to travel to Bali and, indeed, a number of embassy staff had been visiting the island the weekend of the bomb.33

This shared strategic threat analysis was perfectly reasonable on the basis of past experience. It first pointed to communal violence as the biggest danger and then, with increased evidence of terrorist activity, to diplomatic establishments as the most likely targets. There was no basis within this analysis for a more accurate tactical warning that would have turned tourists away from Bali. The problem was not therefore simply one, as has been argued, of political and commercial interests taking precedence over terrorist warnings.34 Such pressures did, however, exist. Anyone checking the website of the American-owned Bali Discovery Tours prior to 12 October, for example, would have found a campaign being waged against the established travel advisories that already urged caution. In December 2001 the US
A later message on the site praised the ‘remarkable finesse of Indonesia’s President Megawati Sukarnoputri, managing to take concrete steps against terrorism without inadvertently bolstering endemic radical fundamentalist movements’, and noted that this effort went ‘seemingly unnoticed and unappreciated by Washington’s policy makers’. It charged that State Department used ‘travel advisories to whip Indonesia and other countries into shapes more acceptable to the Bush Administration’, though they ‘offend the dignity of this large and independent sovereign nation, very eager to be allies with the U.S.’. It was the case that the American and other Western governments had been pressing the Indonesian government to clamp down on JI. Little had been done as a result of the recent return to democracy, a restricted legal framework, and the opposition of the largest Muslim party.38

The attack on Bali led to a revised strategic analysis, which highlighted the possibility of repeat attacks, and to revised travel advice. Britain urged nationals to consider leaving Indonesia unless their presence was essential; ‘extreme caution’ should be exercised in public places; do not feel secure even after high-profile arrests because of the potential reaction from supporters. Australia cautioned specifically against ‘sweeping’ operations [raids] by militant Islamic groups against bars, nightclubs and other public places’ that might particularly aim for Australians. US government personnel in non-emergency positions and all family members were ordered to leave Indonesia,39 while other citizens were urged to depart or to defer travel plans.40 In addition to warnings against travel to Indonesia in general and Bali in particular, all of Southeast Asia was now included. Britain warned in late October that while Thailand was generally ‘trouble-free’, following
‘recent developments . . . UK nationals world-wide should be aware of the risk of indiscriminate attacks on civilian targets in public places, including tourist sites’. The threat to the Thai island of Phuket in particular was said to have ‘increased significantly’. The Australians and Americans also drew attention to this new risk.41 This raised exactly the same tensions that had been evident with regard to Indonesia prior to 12 October between the desire of governments to alert their populations and the dismay of those who depended on tourism for their livelihood. Because of the heightened interest in the role of warnings following Bali those issued at this time were subjected to much more scrutiny.

The new warnings were widely seen as an overreaction, ‘heavily influenced by the domestic political concerns of governments seeking to protect themselves against charges, in case of another attack, that they did not take all precautions’.42 The Thais claimed that there was no evidence of terrorist activity in the area, other than three small groups operating in the country’s four southernmost, and more Islamic, provinces, but that they were checking and improving security.43 The Foreign Minister observed that foreign governments issued ‘advisories based on the first information they receive, not on exclusive intelligence, which is causing panic’.44 On 4 November 2002 the leaders of the ten Association of Southeast Asian Nations (ASEAN) held a summit, along with China, Japan, South Korea, India and South Africa, and issued a statement attacking travel advisories, saying that they only helped achieve the objectives of the terrorists. ‘We call on the international community to avoid indiscriminately advising their citizens to refrain from visiting or otherwise dealing with our countries, in the absence of established evidence to substantiate rumours of possible terrorist attacks.’45

TAKING WARNINGS SERIOUSLY

The Bali episode exercised an important influence on thinking about travel advisories. As forms of risk communication they had serious disadvantages: they tended to be inclusive rather than selective, so governments could not be accused of failing to warn, yet phrased in general rather than specific terms. Americans, for example, were told in 2000 that more than a quarter of the world’s countries were – for one reason or another – deemed to be possibly unsafe for Americans to visit. This included the United Kingdom, a country where ‘terrorist threats and other relatively short-term conditions . . . pose significant risks or disruptions to Americans’. There was an advisory on 15 March 2001 pertaining to the outbreak of foot-and-mouth disease. This tendency to exaggerate the dangers of foreign countries, even when compared with those present in everyday life in the United States, undermined their credibility.46 Bruce Hoffman of the RAND Corporation noted in April 2001
that while on average 26 Americans had been killed per year by terrorists
since 1968, ‘in 1999, the year of the Columbine massacre, this figure was just
two persons fewer than the 28 students killed nationwide in America’s
schools’. He argued that assessments of terrorist threats should be undertaken
‘soberly and analytically lest we overreact, fail to place terrorism in the
context of the many other risks and threats that exist and thereby
inadvertently succumb to the fear and intimidation that is precisely the
terrorists’ timeless stock and trade’.47

Warnings such as those covering Phuket could be said to be discrimina-
tory. One travel agent remarked that: ‘It’s a bloody joke. You have no travel
advisories for Spain, where Basque terrorists stage attacks, but you have them
for Laos, Burma and Thailand, which are among the safest places in the
world for tourists.’48 They could also be said to be ineffectual. One report
indicated that the Phuket warnings had ‘largely been ignored by tourists’.49
This corresponded with wider research conducted by the FCO which found
that few people were aware of the risks to which they might have been
exposed in their previous international trip and most got their advice by
‘word of mouth’. Only two per cent had consulted the FCO or a consulate
overseas.50 Concern that the warnings were being ignored led to proposals in
Australia for agents to provide mandatory summaries of adverse travel
advisory information to customers.51

In Britain the official response was to reappraise the whole system. Foreign
Secretary Jack Straw urged care in the ‘way in which we issue the warnings
and the currency that we thus establish’. It was unwise to act on ‘unassessed,
raw intelligence, some of which is presented to us precisely because it is
inaccurate’. This could ‘shut down economic and social activity throughout
the world, which is exactly what the terrorists want’. He warned of how
terrorists would aim to manipulate the intelligence process by feeding
information that might compromise a source or ‘direct law enforcement
resources to the wrong place’. The raw intelligence has to be ‘skilfully and
carefully assessed before judgements can be made upon it’.52 This view
influenced his response to the ISC report on Bali which recommended greater
clarity in warnings to travellers.53 Straw restated the familiar dilemma: ‘we
have to ensure that travellers are warned of threats that we assess to be
credible, while not causing panic by over-reacting to unsubstantiated pieces
of information.’ In addition, transparency in threat assessments would
provide clues to the terrorists about what was known about them.54

The FCO developed a phased approach to crises.55 A system of strategic
rather than tactical assessments was adopted. Blanket warnings against travel
to an area would be used only when the threat to British citizens looked
‘acute, large-scale and specific’. Straw argued that fewer warnings would
result in the public taking those that were issued more seriously. It would also
reduce the transference of risk. Even tame warnings led tour operators to pull out of destinations and insurers to suspend cover to independent travellers.\textsuperscript{56} Instead of warning ‘against travel to all countries in which there is a risk of terrorists operating’, which would include a large proportion of the world, where there was evidence of risk the FCO would urge ‘common sense’ precautions.\textsuperscript{57}

This set the path for the development of warnings on domestic terrorist threats. Not long after Bali, the Home Office released a document that warned that al-Qaeda could strike Britain with traditional terror tactics or new, ‘surprising’ methods. These might include ‘a so-called dirty bomb, or some kind of poison gas; maybe they will try to use boats or trains rather than planes’. Barely an hour later it was withdrawn and replaced by a more general warning of ‘ever more dramatic and devastating attacks’, observing that: ‘If al-Qaeda could mount an attack upon key economic targets, or upon our transport infrastructure, they would.’ When queried, the Prime Minister’s official spokesman said there had been an ‘administrative slip-up’. The original advice was withdrawn because the government did not want people to be diverted by a specific type of threat. Threats came in different forms, he said, and the public needed to be aware ‘across the range’.\textsuperscript{58}

The Prime Minister addressed the issue in a major speech in November 2002. He described the variable quality of the information received by the security services. ‘Some of it will be reliable; some of it may be misinformation being fed in to waste our time chasing shadows. Some of it will be gossip.’ He worried about the dilemma of ‘warning people with alarming them; taking preventive measures without destroying normal life’. The approach was therefore to act on specific intelligence ‘without causing unnecessary hardship or alarm to the public’ and avoiding general warnings. Shutting down all the places that al-Qaeda might be considering for attack ‘would be doing their job for them . . . If a terrorist thought that all he had to do to shut down the travel industry for example was to issue a threat against our airports, we really would be conceding defeat in the war against terrorism.’\textsuperscript{59}

In March 2003 the Home Secretary made a commitment to provide further ‘clear, accessible public information on terrorism’. A new website (www.homeoffice.gov.uk/terrorism) was launched to provide a range of information from details of terrorist organizations to guidance on personal protection. This was justified in terms of the public’s ‘right to know’ to a level consistent with national security. Only when there was strong evidence and something the public can do should there be a specific warning.\textsuperscript{60} On 30 April 2004 an expanded MI5 website went live and included ‘expert advice to help organisations protect themselves against security threats’.\textsuperscript{61} Home Secretary David Blunkett explained: ‘We are not in the business of rushing in to issue alarmist guidance which in practice does nothing to help ensure
public safety.’ In an August 2004 newspaper article, Blunkett implicitly criticized the American approach, which had just led to a dramatic rise in the alert status. The British assumed that without a high degree of specificity warnings risked causing unnecessary alarm and even panic in the short term but also, if nothing happened, a loss of credibility over the long term. There was a ‘potential risk of inviting ridicule’.62 The policy was to orient the public to potential dangers by sharing a strategic threat assessment rather than regular, but non-specific tactical warnings. Yet the British did not abandon alert levels altogether, maintaining them as guidance for agencies required to deal with security and for conversations with foreign governments. In June 2003, the Joint Terrorism Analysis Centre was established.63 A more complex series of threat levels was introduced, with seven grades. The top four were: substantial, severe general, severe specific, and imminent.

THE AMERICAN SYSTEM

The American approach was quite different. The starting point was the shock of 11 September 2001. The 9/11 Commission Report provides a full and detailed account of the faltering efforts of various agencies to understand what al-Qaeda was up to or to pick up on the various hints of terrorist activity. The panel records that although during the summer months of 2001 the system was ‘blinking red’, and while various alerts appear to have been issued to FBI offices, there was no warning of the dangers facing Americans.64 This statement is not wholly fair. Attempts were made to alert Americans to increased dangers. These dangers, however, were largely believed to be abroad.

The State Department’s Bureau of Consular Affairs issued travel warnings, recommending avoiding travel to a certain country, of which there were about 20–25 in place at any given time. With regard to terrorist threats worldwide caution public announcements were preferred. These covered short-term events, such as ‘coup[s], bomb[es] threats to airlines, violence by terrorists and anniversaries dates of specific terrorist events, and violent demonstrations during elections in a particular country’.65 They were introduced after the bombings of the US embassies in Nairobi and Dar es Salaam in 1998 in order to ‘alert Americans generally to the fact that terrorists have threatened action against Americans and American interests abroad’. Cautions of this type were issued on 5 January and 29 May 2001. This later alert referred specifically to ‘extremist groups with links to Usama Bin Laden’s Al-Qaida organization’, and noted their lack of discrimination between official and civilian targets.

Though the threat was abroad the prompt was potentially at home. This alert was related to the guilty verdicts announced against the defendants in the case of US v Bin Laden. This indicates a feature of alerts that still
continues—the sense of vulnerability emerging out of known events rather than hard intelligence. So on 21 June 2001, 14 individuals were indicted by a US grand jury on charges of murder and conspiracy resulting from the 25 June 1996 bombing of the Khobar Towers military barracks in Dharhan, Saudi Arabia. Although again there was no evidence of any specific threat resulting from this indictment, the next day the previous warning was reissued. On 7 September 2001 it was reissued again, with an additional mention of threats, presumably unrelated to al-Qaeda, to Korea and Japan. ‘Over the last several months, the U.S. Government has learned that U.S. citizens and interests abroad may be at increased risk of a terrorist action from extremist groups.’

There was no system in place for issuing warnings of imminent terrorist attacks in the US. These began after 9/11, demonstrating a degree of improvisation. The government was itself still unsure about the risk and assumed a low tolerance for excessively complex messages. The Federal Bureau of Investigation (FBI), the Attorney General (John Ashcroft) and the new Director of Homeland Security (Tom Ridge) were all involved in making announcements and describing policy. The new Department of Homeland Security was established to fill the need for an ‘institution primarily dedicated to analyzing systematically all information and intelligence on potential terrorist threats within the United States’.

In March 2002 a Homeland Security Advisory System was introduced ‘to provide a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to Federal, State, and local authorities and to the American people’. This set a number of graduated ‘Threat Conditions’, each linked to the measures to be taken by government departments and agencies, and identified with a colour. Green is the lowest, moving through blue (guarded), yellow (elevated), orange (high) and red (severe). According to the Presidential Directive: ‘The decision whether to publicly announce Threat Conditions shall be made on a case-by-case basis by the Attorney General in consultation with the Assistant to the President for Homeland Security. Every effort shall be made to share as much information regarding the threat as possible, consistent with the safety of the Nation.’

After it was introduced the threat condition was normally on yellow (elevated) but there were six periods during which it was raised to high alert—orange. The US was on orange alert for 98 days during 2004, from the start of August through to the presidential elections. The average length of the previous five alerts was 17.4 days. It was never expected that it would go to green or even blue, as that would suggest a controversial level of complacency, while a move to red would invite controversy of a different kind.

Raising the ‘threat condition’ transferred responsibility to federal and state agencies and local law enforcement, and also to individuals. Yet the possible
responses of members of the public do not necessarily suit the authorities. While warning Americans that they might be in danger they also wish to encourage them to act as if they were not. The message, according to one official was: ‘Be scared. Be very, very scared. But go on with your lives.’ After 9/11 a return to normality required assurance that the transportation system, and in particular air travel, was safe. On 1 October 2001 White House spokesman Ari Fleischer was asked about the apparent contradiction between the warnings issued by Attorney General John Ashcroft, including not being able to rule out plans for hijacking additional aircraft, while the President was saying, ‘Get back to work, America; get up in the skies.’ Fleischer responded that the purpose of drawing attention to threats was to encourage people to be alert while moving forward with measures to improve airline safety. President Bush, in a news conference of 11 October after a new alert had been issued, urged Americans ‘to go about their lives, to fly on airplanes, to travel. To go to work.’ The purpose of the alert was to assure them that the government was taking care. Later he added: ‘We cannot let the terrorists achieve the objective of frightening our nation to the point where we don’t conduct business or people don’t shop.’

SOURCES OF ALERT

The administration message from the start was that future terrorist attacks were possible. The first special alert came on 24 September. The particular focus was the possibility of attacks using crop-dusting aircraft to distribute chemical or biological weapons, following information that Mohamed Atta, one of the suspected 9/11 hijackers, had been finding out about such aircraft. Once it became clear that US-led forces were likely to mount attacks against al-Qaeda/Taliban positions in Afghanistan, concern grew about possible retaliation. US intelligence officials reportedly believed that Osama bin Laden had ‘long ago’ begun ‘orchestrating a significant terrorist counterpunch to the expected U.S. retaliation for the attacks on New York and the Pentagon’. An anonymous official was quoted as saying that ‘He has gamed out the next two or three moves already. He expects us to respond to the World Trade Center, and he has the next move planned after that’. The Washington Post reported that ‘credible new information’ had led the FBI and the CIA to assess ‘the chances of a second attempt to attack the United States as very high’ – indeed one intelligence official was said to put the chance at ‘100 percent’ should the United States strike Afghanistan. The potential targets could be in their ‘hundreds or thousands’, from government buildings to ‘centers of entertainment’ to natural gas lines, power plants and other examples of ‘exposed infrastructure’.

The strikes on Afghanistan, beginning on 7 October 2001, were accompanied by a worldwide caution urging ‘Americans to leave Afghanistan’ and
warning of the possibility of ‘strong anti-American sentiment and retaliatory actions against U.S. citizens and interests throughout the world by terrorists and those who are sympathetic to or otherwise support terrorism’. On 11 October the FBI warned that ‘Certain information, while not specific as to target, gives the government reason to believe that there may be additional terrorist attacks within the United States and against U.S. interests overseas over the next several days.’ The warnings were said to be the result of ‘a CIA analysis of several intercepts and intelligence findings that hint that terrorist acts in the near future could occur’. Another source referred to ‘a steady burst of overheard communications, internet chatter and other indicators’.77

Such assessments were not obviously based on anything more than supposition and did not point in any particular direction—within the United States or against American civilian, commercial and military targets elsewhere in the world. Officials were aware that they could be picking up braggadocio or even disinformation designed to discourage the United States from retaliating. It was noted that prior to 9/11, in June and July, apparent threats from al-Qaeda had led to decisions to abandon some US embassies and move navy ships in foreign ports out to sea. In retrospect it was thought that these might have been disinformation designed to occupy officials’ attention, or to allow operatives to observe American counter-terror methods.78

The quality of information available therefore was poor and, as suggested above, this gave more scope for threat assessments to be influenced by considerations of vulnerability or other political concerns. One report suggested that the Justice Department was only acting out of an ‘abundance of caution’ and concern that otherwise the information was likely to leak out anyway; another that ‘sources have told me not to play this up’, implying that the evidence was no stronger than that in ‘half a dozen of these warnings’ issued over the previous few weeks that had not been made public. As in this case the information seemed to suggest a specific timetable, if something did happen ‘they can at least say that they’ve warned the public’.79

A pattern of alerts without subsequent incident was bound to pose problems of a different sort. After a further warning on 29 October, which referred to ‘information developed’ pointing to a possible attack ‘within the United States and against United States interests over the next week’, opening up a wide range of possibilities, this credibility problem was put to Ashcroft. This led the Attorney General to introduce a new theme—the preventative and deterrent effect of these warnings. If people took them seriously and participated patiently in the additional steps taken by law enforcement authorities, they were ‘very likely participating in the prevention of terrorism and in the disruption of terrorism’.80 Building on this theme, FBI Director Robert Mueller described the alerts as ‘a force multiplier’. According to
Ridge, ‘We’ll never know whether the alert that we gave four or five weeks ago discouraged or frustrated some terrorists from doing something that they had planned.’

This alert came at a tense time. Traces of anthrax had turned up at ten different locations in Washington, including the State Department and the Supreme Court, and there had been an emergency landing at Dulles International Airport after a report of a threatening note aboard the American Airlines New York-to-Dallas flight. Some connections were even made with the imminence of Halloween. Newspapers reported that the alert came after intelligence ‘reached a critical mass’. President Bush telephoned congressional leaders on 29 October. Governors were told that the government had ‘new, credible information of the possibility of another terrorist attack’, but ‘no states were named, no location indicated’. What was being assessed, however, was not so much plans as organization. As a result of the Afghanistan campaign authority was believed to have been delegated down al-Qaeda’s chain of command, ‘perhaps even to individual cells of bin Laden’s al Qaeda terrorist network’ to initiate new attacks. Half a dozen such cells had been identified by the FBI in the United States. This meant that even if al-Qaeda’s leadership was eliminated, and even supposing that some local leaders had been detained in the roundup of nearly 1,000 people since 9/11, other cells could now operate on their own. This was essentially an explanation of why there might still be a risk rather than why an attack might be imminent. When nothing still happened this was put down to increased vigilance rather an absence of threat.

When announcing yet another alert on 3 December, Ridge reported ‘an increased volume in level of activity involving threats of terrorist attacks’. The ‘analysts who review this information believe the quantity and level of threats are above the norm and have reached a threshold where we should once again place the public on general alert’. The information, he said, came ‘from multiple sources’, noteworthy for its ‘volume’ as well as its ‘credibility’. There was no ‘specific connection’ with events in Israel, where there had been a spate of suicide bombings. More important, ‘the next several weeks . . . bring the final weeks of Ramadan’ and important religious observations in other faiths’. These had been times when terrorists had planned attacks in the past. Again nothing happened.

In May 2002, the same sort of reports about increasing ‘chatter’, administration figures spoke of the virtual certainty of future attacks though, as Vice President Dick Cheney put it, there was no knowing whether the attack would be ‘tomorrow or next week or next year’. The ‘when not if’ line was repeated by Ridge while Defense Secretary Donald Rumsfeld asserted ‘inevitably that terrorists would acquire and use, chemical, biological or nuclear weapons’.

On 21 May the FBI reported ‘unsubstantiated and uncorroborated
information that terrorists are considering attacks against landmarks in New York City. There was still no information ‘as to time, date or method of attack’ but, regardless, ‘law enforcement in New York’ was notified.87

There was now growing criticism about the lack of hard evidence and, consequently, of useful guidance, leading to anxiety levels being unnecessarily raised and future warnings being devalued.88 In practice the source of a new alert or a travel advisory appeared to be either a reaction to an actual attack, that might be repeated, assumptions of what ‘I might do if I was Osama bin Laden’, sensitivity to coming events or awareness of a symbolic date. Indeed threat assessments clearly involved paying attention to the calendar: an anniversary (of 9/11), the start of a military campaign (Afghanistan, Iraq), Islamic festivals (Ramadan, Hajj), US festivals (Christmas, Memorial Day), big events (great power summits). With travel cautions, a number drew attention to types of dangers illustrated by events: the murder of journalist Daniel Pearl in Pakistan as an indication of a possible targeting of Americans for kidnapping (February 2002); attacks on churches and synagogues reflecting suggesting that terrorists would seek ‘softer targets’ such as ‘facilities where Americans are known to congregate or visit, such as clubs, restaurants, place of worship, schools or outdoor recreation events’ (July 2002); the first anniversary of 9/11 (September 2002). So the intelligence agencies were looking back to past behaviour or forward to possible future triggers for action.

Gradually a new source of information began to make itself felt, especially after al-Qaeda militants were captured in Afghanistan and elsewhere and subjected to interrogation. For example, a report circulated by the FBI on 23 October 2002 indicated that al-Qaeda might be ‘targeting the U.S. railway sector. The reason for the concern was photographs of U.S. railroad engines, cars, and crossings’.89 There was no obvious reason why this finding should translate into an imminent threat.

In November 2002 the FBI issued a warning to state and local law enforcement agencies (but not the general public) to the effect that al-Qaeda may favor spectacular attacks that meet several criteria: high symbolic value, mass casualties, severe damage to the American economy and maximum psychological trauma. The highest-priority targets remain within the aviation, petroleum and nuclear sectors, as well as significant national landmarks.

That is, there could be a repeat of 9/11.90

On 7 February 2003, the alert status rose from elevated to high; Ridge said this was ‘the most significant’ warning since 9/11. Director of Central Intelligence George J. Tenet told Congress that the intelligence was ‘the most specific we have
seen’, involving ‘plots that could include the use of a radiological dispersal device, as well as poisons and chemicals’. There was talk of al-Qaeda’s efforts to get a ‘dirty bomb’ and use surface-to-air missiles (SAMs) and underwater assault teams. AA Guns were placed around Washington and parking lots were closed near NY airport terminals. As for the public, there was no need to alter plans, but Ridge recommended ‘that individuals and families in the days ahead take some time to prepare for an emergency’. Disaster planning instructions, involving the purchase of ‘a three-day-supply of food and water’ and a battery-powered radio, as well as sealing up a room with duct tapes and plastic sheets against chemical or biological attack, led to a rush on supplies in the shops. Many people prepared for a quick evacuation. Soon Ridge was cautioning against overreaction.

The evidence that prompted this seems to have come from interrogations but there was also increased ‘chatter’ intercepted by American surveillance. It seemed likely that attacks would coincide with the end of the hajj, the Muslim pilgrimage. This was a tense period, with the run-up to the Iraq War (and a few days before the war began the alert was raised again having lowered late in February) and warnings from Bin Laden about the dire consequences of an American invasion of another Muslim country. In Britain in February armoured vehicles were moved at one point close to Heathrow airport amid fears that SAMs might be used against aircraft departing from or arriving at the airport. It would have been surprising if there had not been plots of various kinds being hatched by al-Qaeda and similar groups over this period.

On 21 December 2003, just before Christmas, the alert level was raised again. Ridge referred to a ‘substantial increase in the volume of threat-related intelligence reports’, suggesting the possibility of threats around the holiday season. The context was an increased level of global terrorist activity, ‘blood-curdling threats’ on al-Qaeda websites and broadcast by bin Laden’s deputy Ayman al-Zawahiri, past precursors to attacks, and a sense that the US was ‘due’ another attack soon. The specific proposition was that a foreign airliner or cargo jet, possibly flown by an al-Qaeda agent, might be hijacked and crashed into a high-profile US target. Once again anti-aircraft batteries were set up in Washington, with combat air patrols flying above. According to Donald Rumsfeld: ‘You ask, “Is it serious?” Yes, you bet your life. People don’t do that unless it’s a serious situation.’ Soon Air France flights were being grounded. Only on 2 January 2004 was it admitted that this was a case of mistaken identity.

2004 offered a number of high-profile and well-attended events, at home and abroad. On 19 April Ridge spoke of ‘a season … rich with symbolic opportunities for the terrorists to try to shake our will … They plan and prepare and so must we’. The NATO summit at the end of June would be in Istanbul, where there had already been a number of anti-Jewish and anti-British incidents. A plot to attack the summit reportedly had already been
disrupted. The organizers of the Greek Olympics were clearly worried that the games offered a natural target. Timing clearly was important to al-Qaeda but the message was not always straightforward. Take the most significant attack of 2004 outside the Middle East—the 11 May attack on Madrid’s railway network that killed some 200 people. The timing had a symbolic quality (911 days after the 11 September 2001 attack on the US) but it was also days before the Spanish general election, and this could be seen as either an indication that al-Qaeda’s grand strategy was to pick off America’s allies first or to unnerve the Americans prior to their November presidential elections. Al-Qaeda’s own commentary suggested that they were seeking to undermine support for the US in Europe, but this in itself may have been an opportunistic response to the Spanish reaction.

During the 2004 US election the ‘war on terror’ was a central issue in the campaign, yet the authoritative discussion of the terror threat posed to the US was in the hands of senior figures close to the President. Concerns that the administration might seek to scare the population into supporting Bush were raised when, on 27 May 2004, Attorney General Ashcroft asserted that al-Qaeda intended ‘to hit the United States hard’. Seven named individuals were identified as being dangerous, but these were not new names. Two had already been indicted by a US court for alleged involvement in the 1998 bombings of US embassies in east Africa. A claim that an al-Qaeda spokesman had ‘announced’ that plans for an attack on the US were 90 per cent complete turned out to be drawn from the website of a group without any known operational capability and a tendency to claim responsibility for any event that discomfited the US. It was reported elsewhere that no more than a dozen people in the US were being followed as potential terrorists. Officials suggested that the purpose of the announcement had been to ‘reacquaint the public with the risk of terrorism as the summer began’. At any rate the alert level was not raised, and Ridge acknowledged there was not a ‘consensus within the administration’. In July it was Ridge who was warning of plans to ‘disrupt our democratic process’. The alert was not raised because of the lack of precise information.

When the alert was eventually raised, on 30 August 2004, just after John Kerry’s acceptance speech at the Democratic Convention, this was said to be based on new evidence. Out of a joint intelligence operation involving Britain and Pakistan came information that al-Qaeda had developed targeting information, including traffic patterns and structural weaknesses, on financial targets in the US and London. Brushing aside the British government’s reluctance to undermine intelligence-gathering by going public with the information, the Bush administration took the view that this was vital. This was, as Ridge put it, ‘new and unusually specific information about where Al-Qaeda would like to attack’. In presenting this as an imminent threat, Ridge
plugged the President’s anti-terror policies. It was ‘sobering’ to learn about the intent, plans and methods of ‘our enemies’, but the fact that such information was available was ‘the result of the president’s leadership in the war against terror’. Police carrying machine guns began patrolling streets and subways around the targets as well as the area around Capitol. Yet the alert status was raised before much of the evidence had been scrutinized, and it soon became apparent that the suspicious information had been gathered by al-Qaeda well before 9/11. It might have been the case that the plot was lying dormant but the official measures taken were clumsy and sent confused signals. Soon most of the affected roads were re-opened, and the armed police withdrawn.

A detailed investigation published by the New York Times a week before the vote concluded that there was little evidence of a plot linked to the presidential election. The quality of the threat analysis was not given high marks. According to one counter-intelligence official, ‘on a scale of one to a hundred, I’d give it about a two’. The main influence on American assessments had been the Madrid bombings. There was no other supporting information, other than an informant who had been discredited. Non-American agencies reported little to support the view that there was a threat. In the event the November election passed off without a further attack—the only surprise being a belated video intervention by Osama bin Laden that stopped short of endorsing either candidate.

CONCLUSION

The consequences of an ‘orange alert’ in the US were significant: surveillance cameras were activated; first responders were put on alert, police leave was cancelled and officers were required to carry biological and chemical protective masks; patrols were increased on mass transit systems and ports and security checks were increased in sensitive areas. According to the US Conference of Mayors periods of heightened alerts raised security costs by some $70 million a week. Not surprisingly therefore some states and cities decided to opt out unless they could be shown that they were really at risk. Officials in Washington DC, for example, complained about the impact of various alerts on tourism, and cancellation of school trips to the capital. Traffic congestion and stock market reactions were cited as other reasons for ignoring specific warnings sent by Homeland Security.

All this reflected a widespread lack of trust. This meant, according to one high-level report, that ‘The Homeland Security Advisory System has become largely marginalized.’ The system was unable ‘to generate actionable warning of potential or imminent terrorist attack’, thereby frustrating frustrate
federal, state, and local officials and ‘further contributing to the reactive nature of
the U.S. posture vis-à-vis terrorism’. After he left Homeland Security Ridge
indicated that his sensitivity to these costs meant that he was reluctant to raise
the alerts, and that he often clashed with other members of the government. ‘More
often than not we were the least inclined to raise it’, he told reporters. ‘Sometimes
we disagreed with the intelligence assessment. Sometimes we thought even if
the intelligence was good, you don’t necessarily put the country on
[alert] . . . There were times when some people were really aggressive about
raising it, and we said, “For that?”’ His successor Michael Chertoff indicated
his own lack of attachment to the system.

Polling evidence suggested that the alerts had an immediate but temporary
impact. They increased ‘public alertness to the possibility of a terrorist attack’,
but the effects generally lasted about one week, after which people reverted to the
previous prevailing level. In addition, the extent of the increase might have
reflected the low baseline of concern prior to the warnings. After 9/11 or before
the Iraq War, for example, the risks seemed more evident. People did not need
alerts to make them aware of the danger. The most important influence on
perceptions of risk was recent events which provided vivid corroboration of the
dangers. The expectation of future acts of terrorism in the US, for example, went
to over 80 per cent after 9/11 and then subsided by the end of the year to over 60
per cent and went down to just over 50 per cent by the spring of 2002. It then
increased in the spring of 2002 and rose steadily after Bali to close the year at 70
per cent. Over this period, only a minority made any of the government-advised
preparations.

There was scant evidence of panic, even when an understandable sense of
worry led to prudent behaviour. Panic, in the sense of ‘highly individualistic,
competitive, headlong flight behavior’, is habitually exaggerated as a
phenomenon in disasters. Studies after 9/11 noted that ‘concern . . . was
more pervasive than feelings of fear and anxiety’. The risk of future terrorism
was ‘appraised as high, and some reacted emotionally to this prospect, the
numbers were not extensive’. There is little evidence to support claims that
the warnings by themselves create a ‘pre-traumatic stress syndrome’ as
citizens ride ‘an emotional roller coaster without . . . clear instructions on
how to soothe their jitters’. The problem with the warnings was not that
they caused panic but that they became discredited and even risible.

Vague and general exhortations to be alert and vigilant tend to be
disregarded. These are not messages that improve through repetition,
especially when it is assumed that there is not much that can be done. The
public expects government to take responsibility for these matters, unless
there is truly practical advice available. The most important moment for
advice comes after attacks, when timely and accurate information from a
trusted source can make the difference between public anxiety and assurance,
and it is important that the government has not become undermined as a reliable and authoritative source because of the mismanagement of the alert system prior to an attack.  

This diagnosis was widely accepted but the pressure for reform pointed consistently towards greater specificity, with the aim to designate more clearly the regions, cities and types of target most at risk. Between 60 and 70 per cent of state and local organizations surveyed by RAND for the Gilmore panel wanted ‘additional information about the threat (type of incident likely to occur, where the threat is likely to occur, and during what time period) to help guide them in responding to changes in the threat level’. Those drawing on the wider literature on planning also pointed to the requirement for clear, consistent and useful forms of risk communication. When the alert system was reviewed by Congress at the start of President Bush’s second term, with Chertoff now in charge of Homeland Security, there was general agreement that this system should be used less often. A congressional bill to set priorities for Homeland Security was going to make the colour-coded system optional. The requirement now was that ‘Timely and accurate analytic products have to reach’, the responsible state, local, and private sector officials ‘routinely, reliably, and in readily usable form’.

The rough justice of color coding threat conditions for the entire nation must yield to a more sophisticated warning system. This legislation will move the Department of Homeland Security to make regional and economic sector-specific warnings. It will require that threat warnings also convey useable information on protective measures and counter-measures.

This takes us back to the standard described at the start of this article for ‘specific, consistent, accurate, and clear information at the threat at hand, including the nature of the threat, location, and threat time frames’. Yet as Michael Wermuth of the Gilmore Panel pointed out, ‘any alert system will only be as effective as the intelligence upon which it is based, making that function especially critical in this context’. Wermuth then spoke of this problem as if it was one of coping with vast amounts of material and separating true ‘signal from background noise’.

I have argued in this article that the signals are bound to be weak and irregular. If this is the case then it is unrealistic to expect that an alert system can be developed that begins to meet the exacting standards set for reliability, specificity and utility. As one report noted, ‘even supporters of what is known as the Homeland Security Advisory System admit that the system is more art than science—much more—and that the analysis of often scant intelligence and decisions about whether to alert the public to its
Many alerts appear to have been based on suppositions about potential vulnerabilities and what terrorists might do rather than hard evidence of intentions. Other than the evident desire of al-Qaeda and its affiliates to hurt the United States, these warnings have not been informed by a consistent analysis of terrorist objectives, methods and capabilities. They have offered a series of disconnected tactical assessments based on hunches and snippets of information. If there has been an underlying and more sophisticated strategic analysis it has not been shared.

A more strategic approach might encourage improved preparedness for future contingencies by enabling people to assess specific information at times of crisis. If the broad themes of a strategic analysis are internalized, the public may be able to contextualize events when they occur. But it could also have its own problems: the analysis may either be underdeveloped, offering no more than a series of obvious points, or overdeveloped, focusing too rigidly on a particular set of contingencies. Good strategic analysis only appears relatively straightforward in comparison with attempts to develop helpful tactical warnings.

Further difficulties with warning systems were illustrated by the July 2005 bombings in London. The first attack was comparable to Madrid, although less deadly, in attacking the transport system. The timing was possibly linked to the Group of Eight summit taking place that day at Gleneagles in Scotland, although there was no particular reason for the attacks exactly two weeks later against the same types of targets. Although the attacks were quite amateurish, to the extent that the bombs used in the second round fortunately failed to explode, when combined with frantic and intensive police activity and a number of false alarms, they certainly succeeded in raising the anxiety levels around London. A hitherto unknown group claimed responsibility, asserting that London was ‘burning with fear, terror and panic’ in retaliation for Iraq and Afghanistan and warned Italy and Denmark that they should withdraw their troops from Iraq lest they face a similar fate. This claim could not be verified. The bombers themselves left no explanations.

Prior to these attacks, the British government had concluded that generalized warnings were of little value. It issued a booklet to householders offering advice on how to cope with a variety of disasters, and at times instigated rather drastic measures when it believed that a specific target (such as Heathrow airport) was at risk, but it did not follow the American system of alerts. It relied instead on a strategic analysis, though this was not, in its public form, particularly sophisticated and there was a tendency to dramatize the threat in order to gain support for specific policies. Meanwhile, some indications of degrees of anxiety could be found
in the alert levels developed for internal purposes for distribution around the counter-terrorism agencies. Although the Conservative Party has criticized the government for not sharing material on internal analyses with the public, it was known that the alert level had been reduced by the Joint Terrorist Analysis Centre in June from ‘severe defined’ to ‘substantial’, just above the ‘moderate’ risk assigned to Irish Republicans. This reflected some sort of signal that a period of increased danger was over, following the general election (which al-Qaeda might have attempted to influence) as well as recognition that there was no specific intelligence concerning planned attacks (this followed the successful thwarting of a series of planned attacks). It also reflected a degree of confidence that al-Qaeda would find it difficult to mount an attack from outside the UK, although there was also increasing concern at the risk from home-grown militants.

While public statements from British counter-terrorism chiefs were in no sense complacent, they were also reassuring with regard to the level of competence of their organizations and their ability to prevent the most damaging attacks. There is no evidence that the lowering of the alert level had any affect on the ability to pick up signs of the coming attack or the quality of the response. Yet the timing, after years on the same level, seemed unfortunate. At the same time, after months of not raising the US alert level, Homeland Security suddenly introduced an orange alert ‘for the mass transit portion of the transportation sector’ implying that all of a sudden there was a new danger of what has always been one of the most likely forms of attack.

Attempts to bring a degree of specificity to warnings of terrorist attacks are extremely hard to get right. Any moves which betray a lack of urgency will be shown up by an attack and might lead to recriminations: on the other hand, conspicuous moves in alert levels but no attacks can also cause problems, as they will soon be discounted or else provide opportunities for hoaxers. In the circumstances of a long campaign, against a radical, global but also decentralized movement, it will always be hard to be sure about the precise state of the enemy’s plans. Available intelligence should be disseminated to those best able to use it. There may be occasions when a tactical warning is appropriate but they will be few and far between. In democracies it is important that governments do their best to keep people informed but there is no need for every piece of information, however menacing in its implications, to be turned into an alert.

It is reasonable to suppose that there are individuals and groups that are sufficiently organized and determined to be able to mount terrorist attacks against Western countries. They have tried, and succeeded, before and will try again. This is an issue that governments must address and discuss with their people. There are good reasons for encouraging debate about appropriate policies for dealing with this threat, from the organization of the security services to military action to attempts to address ‘causes’.
quality of the prevailing strategic analysis of the terrorist threat is as proper a subject for debate as the prevailing assessment of the Warsaw Pact threat was during the Cold War. Out of this might emerge improved assessments but as valuable will be an improved public understanding of the difficulties inherent in making these assessments.

NOTES

Professor of War Studies, King’s College London. This study has been made possible by a grant from the Economic and Social Research Council. I am grateful for comments from Ragnar Loftstedt, Ben Sheppard, John Stevenson and Simon Wessely.

1 Intelligence and Security Committee, Inquiry into Intelligence, Assessments and Advice prior to the Terrorist Bombings on Bali, 12 October 2002, December 2002, Cm 5724.

2 See for example Baruch Fischhoff, ‘Risk Perception and Risk Communication’, in D. Kamien (ed.), The McGraw-Hill Handbook of Terrorism, in press. Fischhoff considers issues such as smallpox vaccination, surveillance and decontamination.


6 This reflects Tom Schelling’s definition of the ‘game of strategy’ in the Strategy of Conflict (London: OUP, 1960).

7 Malcolm Gladwell, ‘Connecting the Dots: The Paradoxes of Intelligence Reform’, The New Yorker, 10 March 2003, p.86.


16 In Britain, for example, senior police officers treasure their independence and will provide their own assessments of threats which do not always accord with those of

17 *Beyond Bali: ASPI’s Strategic Assessment 2002* (Australian Strategic Policy Institute, 2002), p.3.

18 See Frank Gregory and Paul Wilkinson, ‘Riding Pillion for Tackling Terrorism is a High-Risk Policy’, ISP/NCS Briefing Paper 05/01 (Royal Institute of International Affairs, July 2005).

19 Furedi, ‘Refusing to be Terrorised’ (note 12), pp.13–15 gives a number of examples.


21 Leonie Huddy *et al*., ‘The Consequences of Terrorism: Disentangling the Effects of Personal and National Threat’, p.505.


23 There are claims, based on one particular document, that al-Qaeda decided in 2003 that Spain was the weakest link in the pro-American coalition in Iraq. The fact that this attack led to the defeat of the conservatives in Spain, and the election of a government hostile to a Spanish military role in Iraq, was taken to represent a notable victory for the Islamist cause (although the election result had much to do with Prime Minister Aznar’s inept and opportunistic response to the first news of the attacks, for which he sought to blame ETA). A car bomb outside the Australian embassy in Jakarta on 9 September 2004 may have been attempting to have a comparable effect on the pro-American governing party in Canberra, up for election at the start of October as well as the Indonesian government, two weeks away from its own election.

24 In Canberra one was established into the ‘performance of the Department of Foreign Affairs and Trade (DFAT) and other relevant agencies of the Commonwealth Government in the assessment and dissemination of threats to the security of Australians in South-East Asia in the period 11 September 2001 to 12 October 2002’, http://www.aph.gov.au/senate/committee/fadt_ctte/bali/. In Britain the Intelligence and Security Committee was asked to examine all the intelligence assessments and advice available prior to the attack. Intelligence and Security Committee, Inquiry into Intelligence, Assessments and Advice prior to the Terrorist Bombings on Bali 12 October 2002, Chairman: The Rt. Hon. Ann Taylor, MP, Presented to Parliament by the Prime Minister by Command of Her Majesty December 2002. On 27 May 2004 the Spanish Parliament formed a commission to investigate the handling of intelligence before the 11 March train bombings.


26 These attacks were reported to include random shooting of Israelis and Americans at hotels across Indonesia, abandoned because it would have only ‘minimal impact’; hijack a civilian aircraft and fly it into an Israeli target; a plot in May 2002 to blow up American naval vessels during US–Indonesian military naval exercises, for which Faruq was trained in planting underwater explosives; a chemical attack using cyanide to be sprayed from perfume bottles. *Sunday Times*, 20 October 2002.

27 The threat included Jakarta, Yogyakarta (possibly seen as the most likely), Kalimantan, Lombok, Bali and Sumatra. The six islands mentioned represent a small proportion of the 6,000 that make up Indonesia, but they cover 55 per cent of Indonesia’s land mass, 40 per cent of the total population and the location of 60 per cent of all western tourists.

28 ‘Rumsfeld downplays bin Laden tape’, CNN, 7 October 2002; White House press briefing by Ari Fleischer, 10 October 2002, White House News. On 6 October a boat packed with explosives hit a French oil tanker off the coast of Yemen and one crewman was killed. On 8 October two gunmen linked to al-Qaeda in Kuwait killed a US marine. In September Al-Jazeera played a recording of what it said was Bin Laden’s voice naming all 19 hijackers from the 11 September terrorist attacks on the United States.
300 non-emergency personnel and all diplomats’ family members left US missions in
Indonesia, as a result of a department order following the Bali bombing.

Jane Perlez and Raymond Bonner, ‘U.S. Says It Told Indonesia Of Plot By Terror Group’,

Senate Foreign Affairs, Defense and Trade References Committee, Inquiry into Security
Threats to Australians in South-East Asia.


Con Coughlin, ‘Was it a Failure of Intelligence?’, Sunday Telegraph, 20 October 2002.


The week after the bomb blast in Bali, Indonesia’s Minister of Culture and Tourism called for a considered approach
by foreign powers in issuing their travel bans and warnings pertaining to the country, on the
grounds that Bali and Indonesia were also victims of the terrorist attacks and that the goal of
the perpetrators was economic disruption, the minister suggested one of the means to fight
the threat of terrorism is to support his efforts to rebuild tourism in the wake of the attack.


Hamzah Haz, chairman of the United Development Party (PPP), Indonesia’s largest Muslim
party, had met with Bashir and played down talk of Islamic violence. He is reported as having
said, after 11 September, that the attacks on New York and Washington would ‘cleanse the sins of
the United States’, Asia Times Online; Dan Murphy, ‘How Al Qaeda Lit the Bali Fuse’, in three
gave President Megawati a 24 October deadline (the date she was due to meet President Bush
at the Asia-Pacific summit in Mexico) to act against terrorists or face a public signal from
Washington that Indonesia was a terrorist haven. An invitation was made to Indonesian
intelligence and police officials to interview Faruq. The next day came the bombings in Bali,

US Department of State, Bureau of Consular Affairs, Travel Warning, Indonesia, 19 October
2002.

US Department of State, Office of the Spokesman, Public Announcement, South East Asia,
2 November 2002.

US Department of State, Bureau of Consular Affairs, Consular Information Sheet, Thailand,
30 October 2002.

Raymond Bonner, ‘Qaeda Meeting in Thailand Reportedly Plotted Attacks on Tourists’,

world/asia-pacific/2360209.stm. Apart from the obvious parallels with Bali, one influence
may have been a January 2002 meeting in Thailand involving al-Qaeda operatives to discuss
attacks on ‘soft’ targets throughout Southeast Asia.

=.-. After the terrible tsunami of
December 2004, there were accusations that the Thai government had played down the risk
of such an event because of the risk to the tourism industry.


‘Protecting American Interests Abroad: U.S. Citizens, Businesses, and Non-governmental
Organizations’, Testimony of Dr. Bruce Hoffman, Vice President, External Affairs and Director,
RAND Washington office, before the Subcommittee on National Security, Veterans Affairs, and
International Relations, House Committee on Government Reform, April 3, 2001.


52 The parliamentary debate was on 21 October 2002: Col. 27.
54 The system had six rankings: imminent, high, significant, moderate, low and negligible. The revised rankings would have new definitions to ‘give greater definition between levels’.
55 3 March 2003: Col. 631. The debate came just after yet another outrage in Mombassa. The opposition noted that the FCO had given a vague warning while the Australians urged ‘non-essential travel to Kenya’ to be deferred and made specific mention of ‘threats against Westerners and Western interests in Mombassa’. Straw noted that the Australians lacked any ‘specific information about the timing, location or method of the possible attacks’.
58 BBC, 8 November 2002.
59 PM speech at the Lord Mayor’s Banquet, 11 November 2002.
62 Observer.
63 According to the MI5 website it operates as a self-standing organization comprised of representatives from 11 government departments and agencies. JTAC analyses and assesses all intelligence relating to international terrorism, at home and overseas, and produces assessments of threats and other terrorist-related subjects for customers from a wide range of government departments and agencies. The work is conducted on a fully collaborative basis, with the involvement and consensus of all relevant departments, http://www.mi5.gov.uk/output/Page65.html.
65 In addition there were consular information sheets available for every country of the world. These ‘generally do not include advice, but present information in a factual manner so the traveller can make his or her own decisions concerning travel to a particular country’.
66 In all these cases standard security advice was issued:

‘U.S. citizens are urged to maintain a high level of vigilance and to take appropriate steps to increase their security awareness to reduce their vulnerability. Americans should maintain a low profile, vary routes and times for all required travel, and treat mail and packages from unfamiliar sources with suspicion. In addition, American citizens are also urged to avoid contact with any suspicious, unfamiliar objects, and to report the presence of the objects to local authorities.’

69 On 11 May 2005 a red alert was issued in Washington DC after a two-seater Cessna 150, which had got lost, was detected heading towards the city. As the alarm was raised major public buildings were evacuated. The plane was diverted to an airfield in Maryland.

71 This is reference to the President’s remarks to workers at O’Hare airport on 27 September 2001. There he praised people who worked in the airline industry—‘You stand against terror by flying the airplanes, and by maintaining them.’ He said that a goal of the nation’s war was to ‘restore public confidence in the airline industry’. The travelling public must be told to ‘Get on Board. Do your business around the country. Fly and enjoy America’s great destination spots.’

72 Ari Fleischer, White House Press Secretary, 1 October 2001.

73 ‘George W. Bush Holds News Conference’, 11 October 2001 The point was reinforced by Ashcroft. The alert, he insisted, ‘should promote caution not incite alarm . . . We are going to be more alert to security at the airports, but we’re not going to cease to fly. We’re going to be more alert in a variety of aspects of our existence, but we’re not going to cease to live.’ ‘John Ashcroft Holds Justice Department News Briefing’, 12 October 2001.

74 Another individual in custody had been downloading information from the Internet about aerial application of pesticides, or crop dusting. ‘John Ashcroft Testifies Before House Judiciary Committee’, 24 September 2001. Minnesota Public Radio on 21 September reported that Hollywood studios were on alert after the FBI warned they could be targets for terrorism. Sony Pictures, Twentieth Century Fox and Walt Disney Company were among the studios that cancelled public tours and installed metal detectors.

75 ‘We know that there are other terrorists out there and that the threats could be growing’, one federal law enforcement official was quoted as saying. ‘What we have to do now is just be prepared.’ It was also reported that a significant number of federal agents were being held back from the current investigation into 9/11 as a reserve in anticipation of possible secondary attacks. This report claimed that this was the ‘first time that the Bush administration has said it believes that Bin Laden and Al Qaeda already have in place follow-up attacks and an infrastructure for carrying them out, *Los Angeles Times*. 30 September 2001.


80 Press Conference with US Attorney General John Ashcroft and Robert Mueller, Director of the Federal Bureau of Investigation, 29 October 2001. FBI Director Mueller said that there was no reason to believe that this new intelligence was related to the anthrax scare.


83 Thanks to the patience and vigilance of the American people, Ashcroft remarked on 8 November, ‘we know this: We have not suffered another major terrorist attack.’ ‘John Ashcroft Delivers Remarks To Justice Department Employees’, 8 November 2001.

84 Ramadan was specifically mentioned on a Bin Laden tape as a time of potential attack.


86 There had been other more specific warnings. In April, Attorney General John Ashcroft warned about possible attacks against banks in the Northeast and in early May US officials informed law enforcement agencies about a possible threat to high-rise apartment buildings, thinking that terrorists might rent an apartment, gradually pack it with explosives, and then detonate it in an effort to destroy the building.

87 In November 2001 the Governor of California had disclosed a threat (for which there was no corroboration) to suspension bridges on the West Coast, which led to heightened security on the Golden Gate Bridge. This was not information that had been thought suitable for publication at the Federal level, and it was later stated that this threat was not credible. *CBS Morning News*, 7 November 2001, SC 12 0231.
The claim that Washington, New York or Florida was about to be hit by a ‘dirty bomb’ turned out to be a figment of the imagination of a captured al-Qaeda member, garnished with a lot of information about means of delivery, including shoes, suitcases and laptops and specific targets. Brian Ross, Len Tepper and Jill Rackmill, ‘False Alarm? Terror Alert Partly based on Fabricated Information’, ABC News, 13 February 2003.

On 29 April, Turkish police broke up an alleged cell of Qaeda ally Ansar al-Islam that they said was plotting to attack the NATO gathering. They arrested 16 men and seized explosives, guns, bomb-making manuals, and videotapes and compact discs featuring Osama bin Laden, according to Turkish officials.


NY Stock Exchange, midtown Citigroup building, Prudential financial Building in Newark, NJ, World Bank and IMF in Washington DC.

Leonie Huddy, Stanley Feldman, Gallya Lahav and Charles Taber, ‘Fear and Terrorism: Psychological Reactions’, in Pippa Norris, Montague Kern and Marion Just (eds.), Framing
In surveys conducted for the Pew Center the 70 per cent of Americans who declared themselves depressed immediately after 9/11 was down to 29 per cent by mid-October, while those having trouble sleeping declined from 33 per cent to 12 per cent (http://people-press.or/midoct01rpt.htm). A Swedish study shows similar results: Lennart Sjöberg, ‘The Perceived Risk of Terrorism’, *Risk Management: An International Journal*, 7/1 (2005), pp.43–61. This experience is confirmed by a survey following the London attacks of 7 July 2005. G. James Rubin, Chris R. Brewin, Beil Greenberg, John Simpson, Simon Wessely, ‘Psychological and behavioural reactions to the bombings in London on 7 July 2005: cross sectional survey of a representative sample of Londoners.’, BMJ, doi: 10.1136/bmj.38583.728484.3A (26 August 2005). This study found increased stress levels, and concern about using the London underground, but little requirement for professional help.

112 Gilmore Report, D-7-2.
118 Patrick Mercer, Shadow Minister for Homeland Security stated that: ‘The Government . . . seems utterly incapable of warning the public about the threat of terrorism.’ *Daily Telegraph*, 12 December 2004. This was prompted by reports of an intelligence analysis that put the al-Qaeda threat as ‘severe’ and suggested as targets military establishments and ‘crowded places or events’. This was said to have created a risk to New Year celebrations. In the US the colour-coded alert system was designed for local government and law enforcement agencies but the view was taken in Washington that as it would be impossible to keep this from the public it needed to be shared.