CHAPTER 30

CONTENTS

Counterterrorism

Paul R. Pillar

Abstract

In this chapter, students will learn about the several different elements involved in combating international terrorism, including dissuading individuals from joining terrorist groups, dissuading groups from using terrorism, reducing the capability of terrorist groups, erecting physical defences against terrorist attacks, and mitigating the effects of attacks. Reducing terrorist capabilities in turn requires the use of several instruments – each with its own strengths and limitations – including diplomacy, intelligence, financial controls, criminal justice systems, and military force. Counterterrorism unavoidably raises difficult and often controversial policy issues, including conflicts with other values such as personal liberty and privacy.

Introduction

The prominence of counterterrorism in recent years and especially during the past decade obscures how old the underlying challenges are. Terrorism dates back to ancient times. Counterterrorism, as a concerted and cooperative effort by governments to combat this tactic, is not that old, but it long predates any 'war on terror' aimed at the Islamist variety of international terrorism that is

the most recent focus of attention. What could be called the first international conference on counterterrorism took place in Rome in 1898, to deal with a wave of anarchist assassinations that had been going on worldwide for several years.

Interest in counterterrorism has waxed and waned throughout modern history. That fluctuation in interest has in part reflected the rise and demise of different types of terrorist threat, such as the anarchism of the 1890s or the leftist violence that beset Europe in the 1980s. It also has reflected the political mood and milieu in individual countries. Terrorist attacks were occurring in the United States in the mid-1970s, for example, at a pace that would cause public alarm if replicated there today. But because the American public then – having just lived through the wrenching Watergate affair – was more concerned about excesses and abuses by its own government, the attacks did not stimulate major new counterterrorist initiatives (Jenkins 2003). Understanding counterterrorism requires awareness of such swings in public mood and attention, but it also requires focusing on the essential elements and issues of counterterrorism that are present regardless of the political environment.

Basic elements

Not everything that can be done to combat terrorism ordinarily bears the label of 'counterterrorism'. Anything that cuts the roots or attenuates the causes of terrorism is properly viewed as being at least partly a counterterrorist measure, even if it is not commonly called that and even if other policy goals are involved. Scholars and politicians often disagree about the roots of terrorism. Some focus on the conditions in which would-be terrorists live. Others point to particular conflicts that become sources of rage. Still others emphasize the allure of extremist ideologies propounded by terrorist leaders and groups. Despite these differences of emphasis, they all have to do with one of the basic elements of counterterrorism, which is to reduce the motivation for individuals to join terrorist groups.

Counterterrorist policies that reflect the different ways of looking at the causes of terrorism mentioned above are not mutually exclusive. A government may, for example, promote political and social change to weaken what it regards as roots of terrorism as well as waging a battle of ideas against extremist ideologies. These two approaches both have been facets of US counterterrorist strategy focused on the Middle East, especially in the wake of al-Qa'ida's attacks in September 2001.

For several European governments, attention to the roots of terrorism has more to do with their own Muslim populations. High-profile terrorist attacks such as those against transit systems in London and Madrid have heightened attention to the status of European Muslims. Here, too, there are disagreements and differences in approach, such as between the British concept of multiculturalism and the French emphasis on assimilation. But in either case, reducing the chance that young members of these communities will gravitate toward terrorism is a goal of government policy.

Another fundamental element of counterterrorism focuses on decisions by groups on whether to conduct more terrorism. It has to do with shaping the incentives for groups to use peaceful rather than violent means to pursue their objectives. This element is not germane to all terrorist groups. It is irrelevant to a group such as al-Qa'ida, whose ultimate goals – overthrow of most of the political order in the Muslim world – are so sweeping they could never be assuaged by any negotiations, concessions, or change of policy by a government. Even with groups whose goals are more circumscribed – as was true of the now-defeated Liberation Tigers of Tamil Eelam and its objective of an independent Tamil state carved out of Sri Lanka – the conflicts of interest may still be so acute that it is extremely difficult to divert the group from its violent path.

In some instances, however, a negotiated resolution of issues in conflict can be a major part of inducing a group to cease terrorism. The most conspicuous case is the Good Friday agreement on Northern Ireland reached in 1998. Despite many fits and starts over the subsequent decade, the peace process centred on that agreement was instrumental in inducing the leadership of the Provisional Irish Republican Army to give up terrorism.

The remaining elements of counterterrorism are more commonly labelled as such. One is usually called 'incident management,' which includes anything done, once a terrorist incident occurs, to mitigate its effects. The concept of incident management first arose in response to attacks in which hostages are seized and their lives are kept in jeopardy as the terrorists voice demands, such as for the release of previously jailed comrades. Management includes communications or negotiations with the terrorists. Expertise has been developed over the years (and has been applied by police services and private security firms to terrorist as well as non-terrorist hostage situations) on how best to deal with hostage-takers. The principal objectives usually are to weaken the will of the terrorists while avoiding any move that could stimulate rash action and harm to the hostages. Ultimately, however, the outcome of such incidents depends heavily on the policy of the authorities involved toward making concessions under duress to terrorists. Some governments (e.g. Italy) have been willing to make concessions in the interest of securing safe release of hostages. Others (e.g. the United States) are opposed to such concessions on grounds that they encourage further terrorism.

Another aspect of managing such incidents involves communications with the public and the role of the press. An objective of terrorists in staging such incidents – at least as much as the specific demands they make – is to gain attention for their cause. Partly because of this, some counterterrorist officials consider it important to restrict the release of information on such incidents and to limit public attention to them. Any such restrictions, however, raise issues of freedom of the press and of the responsibility of the press and government alike to inform citizenry about important events.

A third aspect of management of such incidents is the possible use of force to rescue the hostages. A successful rescue operation avoids the difficult choices of whether to make concessions to terrorists, as well as constituting a dramatic

blow against terrorism and immediate punishment of terrorists. Past failures at hostage rescue have stimulated the development of highly skilled forces trained to conduct rescue operations. Germany developed such a force after its failure to rescue Israeli athletes taken hostage at the Olympic games in Munich in 1972, as did the United States after its aborted attempt to rescue diplomatic hostages in Iran in 1980. Even well trained forces, however, face an extremely difficult task because the terrorists have the advantage of being able to inflict immediate harm on hostages. Because of this inherent difficulty, the record of hostage rescue attempts always will be mixed (see Box 30.1).

In recent years, most major terrorist incidents have involved not the seizure of hostages and the threat of inflicting harm on them, but instead the direct and unprovoked killing of innocent people, usually with bombs. In this context, 'incident management' has come to acquire a different meaning, referring primarily to emergency responses designed to tend to the wounded and to deal with any continuing hazards at the scene of the attack. The underlying purpose is still to mitigate effects of the attack; prompt medical attention for the wounded, of course, can minimize the number of deaths. Particular emphasis is now placed on responding to terrorist attacks using unconventional weapons or materials. Despite what is still the relative rarity of such attacks, the emphasis is warranted because quick measures to contain or neutralize a biological, chemical, or radiological hazard could make a substantial difference in minimizing casualties beyond those sustained immediately in the attack itself.

The measures that are most often thought of explicitly as counterterrorism – and that are the focus of the remainder of this chapter – concern efforts to curb the *ability* of terrorists to conduct attacks. These include defensive security measures designed to protect potential targets from attack. They also include a variety of offensive measures intended to reduce terrorist capabilities.

Defence

Defensive security measures (which sometimes bear the label 'anti-terrorism') are applied at several different levels. Most specific is the protection of individual sites, be they office buildings, military bases, embassies, or any other facility that could become a target of terrorist attack. Much site-specific security is the business of the private sector – of the owners or managers of the facilities being protected. Government facilities tend to have more security per site because the security also serves other purposes (such as preserving the secrecy of sensitive activities) and because in the eyes of terrorists, official facilities are likely to have greater symbolic value as targets for attack. Related types of security include special short-term protection provided to high-profile events such as inaugurations or major sporting events and personal security given to governmental leaders or other prominent persons.

The next level of defensive measures is security provided to entire systems. The systems-level security that has played the greatest role in counterterrorism

BOX 30.1 SUCCESSFUL AND UNSUCCESSFUL RESCUE ATTEMPTS

Attempts to rescue hostages taken by terrorists have ranged from brilliant successes to tragic failures. Some countries have experienced both types of outcome.

An example of how a rescue attempt can go horribly wrong involved the hijacking by the Abu Nidal Organization of an Egyptian airliner in 1985. A team of Egyptian commandos attempted a rescue while the plane was on the ground in Malta, beginning their operation by using explosives to blow open doors of the aircraft. In an ensuing exchange of grenades and gunfire, the interior of the plane caught fire. Fifty-six out of 88 passengers died, as did two crew members.

A conspicuous success ended one of the last of the major hostage takings, which began in late 1996 when the Tupac Amaru Revolutionary Movement (MRTA) seized the Japanese ambassador's residence in Lima, Peru. The Peruvian government negotiated with the terrorists for four months while secretly digging tunnels underneath the residence and making other preparations for a military raid. The raid began with an explosion that collapsed part of the ground floor of the building (where the MRTA members were playing a soccer game, with their 72 hostages being kept on an upper floor). All but one of the hostages were rescued unharmed. Two members of the rescue force and all 14 terrorists were killed.

is that surrounding civil aviation. The inherent vulnerabilities and mobility of airliners always will make them tempting terrorist targets. The protection given to commercial aviation today demonstrates two principles of systems-level security. First, a chink anywhere in the armour can provide an opening for attackers – which is why reported weakness in security procedures at any one airport is legitimately a concern for people elsewhere in the system. Second – and partly in recognition of the first principle – security must be multi-layered, which in the case of aviation includes everything from x-ray inspection of baggage to hardening of cockpit doors. No other systems have received as much counterterrorist attention as aviation, but obvious vulnerabilities have increased questions in recent years about the need for additional protection to other systems such as public transit and electrical power grids. Electronic systems, such as those that support banking and financial transactions, also have received added scrutiny.

The most general level of defensive security measures is the protection of an entire country, particularly by keeping terrorists, and to some extent the wherewithal for conducting terrorist attacks (especially nuclear material) outside its borders. The United States, following the 9/11 attacks, greatly increased its emphasis on homeland security. This included not only a substantial increase in expenditures but also the creation – in the largest US governmental reorganization in over 50 years – of a Department of Homeland Security. The geographic and other circumstances of each country, however, make the homeland security task different for each. For most European countries, free cross-border movement within the European Union would

make it impossible for individual states to approach homeland security in the same way the United States does. (In recent years some border controls within Europe have been reinstated, although more because of concerns about immigration rather than terrorism.) Even the United States, given its long undefended border with Canada, must consider how much emphasis to place on stopping terrorists at its own borders and how much to keeping them out of North America altogether.

Defensive countermeasures work in several ways. The most obvious is the direct foiling of an attempted terrorist attack. Even if defences do not defeat an attempted attack, however, they may deter terrorists from attacking. Terrorist preparations typically include substantial study and surveillance of the intended target, to identify vulnerabilities and possible avenues of attack but also to assess security measures. Sometimes terrorists conclude from such study that the security protecting their intended target is too strong, and they stand down from their planned attack. Of course, this does not necessarily mean that they forgo terrorism altogether; they may look for an alternative target. But at least the defences complicated their planning and forestalled whatever specific objective they had hoped to achieve by hitting their primary target.

Complicating terrorists' planning like this also slows them down, providing more time in which they might be detected. This raises another general way in which security countermeasures work, which is to complement other counterterrorist efforts. Defences that force terrorists to prepare their operation in ways they might not otherwise have used may increase the chance they will be caught. Besides lengthening the time to prepare an attack, another possibility is the need to build a bigger bomb to overcome security such as blast-resistant walls or barriers that create a standoff distance. The purchases and fabrication needed for a larger bomb may be more conspicuous and detectable than the making of a smaller device.

Mention of large bombs raises a final way in which defensive measures can save lives even if they do not prevent attacks. The truck bomb that terrorists used to attack the US military housing facility at Khobar Towers in Saudi Arabia in 1996 was so powerful that it killed 19 servicemen even though it exploded some distance away in the street. In a sense, perimeter security at the facility worked; if the truck had been permitted to enter the compound, the casualty toll would have been far higher.

Defensive security measures have several inherent limitations. They are expensive. The costs are measured not just in direct monetary expenditures for security, although some commonly used methods – such as machines that are both effective and efficient in screening large volumes of luggage of air passengers – are indeed expensive. The less measurable but still significant costs come in the form of unavoidable inefficiencies imposed on the people being protected and higher costs of doing business stemming from such things as longer travel time. Some legitimate business, including government business, may be more difficult to do at all. The type of embassies that can most readily be protected from terrorist attack, for example – fortress-like

compounds located away from city centres – also make it harder for the diplomats who work there to do the parts of their job requiring free and easy interaction with the local population.

The most important limitation is that not everything can be protected, even though everything is a potential terrorist target. Terrorists always will have the advantage of choosing where to attack, with that choice reflecting in part where security is strong and where it is weak. In that sense the strengthening of security countermeasures has a self-negating aspect. Whatever the form of competition, the offence always has this advantage over the defence.

Going on the offensive

Offensive counterterrorist operations have the attraction of not surrendering the initiative to terrorists and not trying to guess where and how they will strike next. A successful security countermeasure saves from attack whatever target or potential target is being protected. A successful offensive operation that puts a terrorist cell out of business prevents it from ever attacking *any* target. This does not mean that offensive operations are an alternative to defensive efforts. Rather, they are complementary parts of a comprehensive counterterrorist programme.

Offensive counterterrorism itself involves the use of several different tools. Again, they are complements rather than alternatives to each other. Each tool has its own advantages and limitations.

The transnational nature of modern terrorism makes *diplomacy* an important tool. Enlisting the cooperation of other governments is critical to countering terrorist operations that cross international boundaries. Diplomacy's most immediate use is to obtain cooperation on specific cases. A diplomatic démarche is the channel through which to get another government to arrest a suspected terrorist, to raid a terrorist cell, or to turn over a suspect. Diplomacy also can help to drive and guide cooperation more generally between military, security, and intelligence services. As such, it provides important support to all of the other counterterrorist tools. Finally, diplomacy is the main means for containing and confronting state sponsors of terrorism.

Counterterrorist diplomacy can be either multilateral or bilateral. Multilateral diplomacy is most useful in creating a worldwide climate that recognizes terrorism as a shared problem and that is supportive of counterterrorist efforts. (Public diplomacy – communication through mass media to publics rather than to governments – also gets used for this purpose.) Multilateral diplomacy has succeeded in making that climate more conducive to counterterrorism than it was a quarter century ago, when much terrorism got overlooked or condoned out of a disinclination to criticize 'national liberation movements'.

Multilateral diplomacy also has a more practical side, in the form of a series of international conventions on terrorism that have been negotiated over the past 40 years and that establish rules and procedures on such matters as jurisdiction over hijacking incidents and the tracing of explosives. Most

practical international cooperation on terrorism, however, is bilateral. Individual terrorist cases typically involve only two or three states at a time, and the handling of secret material becomes more difficult the more states that are involved.

Another tool that diplomacy has been instrumental in supporting is *financial control* in the form of freezing or seizing of terrorist assets. Getting at terrorists' money has received increased emphasis in recent years, although legal instruments for doing so have existed much longer. The United States Treasury has long had the statutory authority to freeze the financial assets of states, groups, or individuals associated with terrorism. Except for states, however – whose financial accounts are more readily identified than those of groups or individuals – the haul of frozen assets was meagre until after 9/11, when the assistance of other governments became easier to obtain. US legislation in 1996 that created a formal list of Foreign Terrorist Organizations also made it a crime to contribute financially to any organization on the list.

Despite frequently expressed hopes of curbing terrorism by removing its 'lifeblood' of money, the contribution of financial controls to counterterrorism always will be limited for two reasons. One is that much of the money associated with terrorist activity flows through channels that are extremely hard to detect and intercept. This is particularly true of the informal money transfer networks known as *hawala* that are prevalent in the Middle East and South Asia. The other reason is that most terrorism is cheap. It simply does not cost much to assemble a truck bomb or many other means of inflicting heavy casualties.

The tool that perhaps has received more emphasis than any other in discussions of counterterrorism is *intelligence* (see Chapter 16, this volume). Inquiries in the United States following the 9/11 attacks focused primarily on intelligence. One of the principal legislative responses to the attacks was a reorganization of the intelligence community that created an additional counterterrorist centre and an additional layer of supervision over the entire community. The sentiment to which such measures are a response has more to do with defence than with offence: the hope that intelligence will uncover enough details of the next major terrorist plot to enable authorities to roll the plot up before it can be executed.

That hope, although an understandable reaction to tragic events and a widespread perception of what intelligence ought to do, is largely misplaced. Unearthing the tactical details of terrorist plots must always be one of the missions of intelligence, and the occasional successes in doing so are among the most satisfying counterterrorist triumphs. But such successes always will be rare. Some terrorist plots, including some major ones, always will go undetected no matter how skilled and assiduous the intelligence operations aimed against them may be. Terrorist plots – which typically involve small numbers of operatives who can conduct their operations in secret, avoid communications or any overt actions that could reveal their plan, are highly conscious of operational security, and are ruthless toward anyone suspected of betraying them – always will be extremely difficult targets for intelligence.

Intelligence performs three other functions that make larger contributions to counterterrorism. One is to provide a more strategic sense of terrorist threats – are they increasing or decreasing, which groups or states pose the greatest dangers, and which areas of operation are of most concern. Such strategic appraisals help to guide policymaking on all aspects of counterterrorism, including security countermeasures as well as offensive operations. A second function is to provide detailed support to all the other tools. Diplomatic démarches about terrorism, for example, nearly always are based on – and very often convey – information collected by an intelligence service. Intelligence also is important in identifying and locating terrorist financial assets. And intelligence provides critical input to law enforcement and military operations, discussed below.

The third function is clearly offensive and in many ways the most important. This is the collection and analysis of information on terrorist organizations and infrastructures, enabling them to be disrupted. The information concerned is specific but not plot-specific. It involves the names and biographic data of suspected terrorists, the location and strength of terrorist cells, the location of safehouses, and the operational connections among cells and groups. Intelligence services themselves might not accomplish the actual disruption, but the information they provide enables police or internal security services to conduct raids, arrest suspects, and confiscate material. Such actions often provide leads for collecting more information, which in turn facilitates further disruption of terrorist infrastructure. This type of offensive action does not always generate headlines, unless a particularly well-known terrorist is taken into custody or killed – as was true of the raid in Pakistan by US special forces in 2011 that killed Osama bin Laden and also involved the seizure of a large amount of exploitable material (see Box 30.2). But it probably accounts for the largest portion of counterterrorist successes, including successes against important groups such as al-Qa'ida.

Law enforcement and military force

A common, but misleading and useless, frame of reference often invoked in discussion of counterterrorism is to ask whether the problem should be considered one of 'crime' or 'war'. Nothing inherent to terrorism warrants either posing such a choice or selecting one of these labels as an alternative to the other. Terrorists clearly commit crimes (such as murder), while their political objectives give them something in common with warfare and distinguish their actions from non-political crimes motivated by greed or passion. Counterterrorist policies and practices also do not provide a basis for any 'crime versus war' choice. Both criminal justice systems and military services appropriately play roles in counterterrorism. The establishment by the United States of military tribunals to determine the guilt or innocence of terrorist suspects – a system that is inseparably part of the realms of both 'crime' and 'war' – illustrates the falsity of the dichotomy.

Most proponents of the 'crime versus war' formulation are really just arguing in code for greater emphasis to be placed on one or the other of the associated counterterrorist tools: *criminal prosecutions* or *military force*. Most often, it is proponents of military force who invoke that formulation, because 'war' has the added favourable connotation of taking the problem seriously and giving it high priority. A more useful perspective, however, is to discard the metaphysical and semantic debates and realize that criminal justice and military force are simply two additional offensive counterterrorist tools. Like the other tools such as intelligence or diplomacy, each tool has its peculiar strengths and weaknesses. And as with the others, they are best used as complements to each other as part of an integrated counterterrorist programme.

Arrest of suspected terrorists and their prosecution in a criminal court can accomplish several things. Incarcerating (or executing) a terrorist obviously prevents him from committing further attacks. A well-publicized prosecution can help to demonstrate governmental resolve. It may also strengthen deterrence of other terrorists apprehensive about getting caught. Even if not deterred, the fear of getting caught may impede or restrict their operations. A successful prosecution can satisfy the public's appetite for punishment of wrongdoers, but does so in an orderly and peaceful framework that upholds respect for the rule of law.

Use of a criminal justice system also has significant limitations. A terrorist first has to be caught, of course, before he can be prosecuted. Senior leaders who plan and direct terrorist attacks are less likely to be caught than underlings who must be at the scene of the attack. In the case of state-directed terrorism, the leaders most responsible are unlikely ever to be arrested. Deterrence may be ineffective – particularly inasmuch as leaders tend to go free – and is irrelevant to suicide bombers. A legal case that establishes beyond reasonable doubt that someone has committed terrorist crimes is more difficult to make than an intelligence case that someone is probably a terrorist. There is thus the risk of acquittal, an outcome less favorable to counterterrorism than if a terrorist had not been arrested in the first place. Accused terrorists may use a public trial as a platform for propaganda. Incarceration of convicted terrorists may stimulate further attacks, perhaps in the form of hostage-taking aimed at bargaining for the prisoners' release.

With terrorists moving and operating across international boundaries, jurisdictional issues also complicate the application of criminal justice. This has partly involved the assertion by the United States of extraterritorial jurisdiction of terrorist crimes against US interests in other countries, an assertion that is questionable under international law and that comes into conflict with the laws of the countries on whose territories the crimes were committed. Disagreements over the death penalty – opposed by the European Union, still used in the United States – have been an added complication that has impeded the extradition of, and even sharing information about, some terrorist suspects.

Some have looked to the International Criminal Court (ICC), the founding statute of which was ratified by enough states to enter into force in 2002, as a

place to prosecute international terrorists while pre-empting some of these jurisdictional issues. There remain problems, however, of distinguishing terrorist crimes to be tried in the ICC from ordinary crimes that would still be tried in national courts. The handling of sensitive security-related information, which is often involved in terrorism cases and is difficult enough to use as evidence even in national courts, is another complication for the ICC.

The most successful use of military force for counterterrorist purposes was the US-led intervention in the civil war in Afghanistan following al-Qa'ida's attacks in the United States in September 2001. Notwithstanding the subsequent continued security problems in Afghanistan (where command of the international forces was later turned over to the North Atlantic Treaty Organization), the intervention did force al-Qa'ida from its main sanctuary and ousted the Taliban regime, which, as a close partner of al-Qa'ida, had become a major state sponsor of terrorism. This success helped to raise expectations, especially in the United States, about how a more aggressive use of military force might be used effectively to combat terrorism.

Some of the principal attractions of military force for this purpose are stronger versions of the attractions of using a criminal justice system. A military strike can be an even more dramatic demonstration of resolve than a prosecution. It can immediately disrupt or destroy terrorist capabilities, such as training camps, and possibly kill key terrorists. It may have deterrent effects not just on terrorist groups but also on states. And it can do all this without the administrative, evidentiary, and other legal complications that often impede criminal prosecutions.

The principal limitation of the counterterrorist use of military force is that international terrorism simply does not present very many good military targets. Afghanistan of the Taliban was a unique case. Even state sponsors in general have become a significantly smaller part of international terrorism than they were two decades ago. And with groups rather than states, most of the important preparations for terrorist attacks occur not in open air training camps but in places not readily targeted for military strikes, such as apartments in cities, including Western cities.

Further limitations parallel some of those associated with criminal prosecutions. A military attack may serve more to provoke than to deter. The US military strike on Libya in 1986 in response to a terrorist attack in Germany may have helped to provoke the much deadlier Libyan bombing of Pan American flight 103 two years later. Being subject to a military attack may rally support for an extremist group's leader, among the group's membership and possibly among a wider constituent population. Military strikes also have their own practical problems, such as access to bases and overflight of third countries.

Other drawbacks stem from the inherently destructive nature of military force. Collateral damage, including the loss of innocent lives, is almost inevitable. Such damage can alienate civilian populations, as it has to some degree as a result of military operations in Afghanistan and missile strikes in northwest Pakistan launched from unmanned US aircraft. Some will always

regard the use of military force as excessive, making it at least as prone to controversy as any other counterterrorist instrument.

Issues and choices

The expansion of counterterrorist powers and functions, even if not involving military force, frequently gives rise to public debate. This in part reflects disagreement over the effectiveness of particular measures in curbing terrorism. It also stems from unavoidable conflicts and trade-offs between counterterrorism and other public values and goals.

The treatment of suspected terrorists has been one focus of controversy in the United States and Europe in the years since the 9/11 attacks. The controversy comes not from any reservoir of sympathy for terrorists but instead from concerns over human rights and the principle that even the guilty should be treated humanely. Another concern is that not all suspects are in fact guilty.

Issues involving the handling of suspected terrorists have spilled over international boundaries and have included reports of secret prisons in which detainees have been held incommunicado indefinitely, as well as 'renditions' in which suspects are turned over from one country's custody to another without any open legal procedure to authorize the process. Renditions have been used for many years as an efficient way to get suspected terrorists to the countries where they are most wanted for their crimes, without the pitfalls associated with a formal extradition process. They have become more controversial largely because some of the receiving countries have been known for their rough handling, including torture, of prisoners. Torture in general, even with detainees who have not been subjects of rendition, also became a more prominent issue of debate in the years. This was especially due to the use of 'enhanced interrogation' techniques under the George W. Bush administration in the United States. The relevant questions include not only whether human rights are being violated but also whether torture is effective in eliciting accurate information.

Beyond torture is the issue of assassinating individual terrorist leaders, often referred to as 'targeted killings'. Some argue that this kind of decapitation of a terrorist group or cell can be effective in preventing terrorist attacks, and that the procedure should not be considered functionally or morally different from many conventional military operations. Others emphasize what can go, and has gone, wrong in clandestine assassinations, including the killing of innocent people through mistaken identity or collateral damage. Moreover, such assassinations may constitute a stooping to the same level as terrorists, by using a procedure that in some contexts can be considered terrorism itself. Both sides can find much to adduce in the experience of Israel, which has made extensive use of targeted killings as a counterterrorist tool (Byman 2006). The killing of Osama bin Laden in 2011 was generally accepted, especially outside Pakistan, as a legitimate counterterrorist measure, given the notoriety of the target and the care that went into planning the operation (see Box 30.2).

BOX 30.2 THE DEATH OF OSAMA BIN LADEN

On 2 May 2011, al-Qa'ida leader Osama bin Laden was killed in a raid by US special forces on a compound in Abbottabad, Pakistan. The raid, in which the US commandos reached the compound by helicopter from Afghanistan, relied on intelligence painstakingly gathered for several years and concluded a manhunt that had lasted well over a decade.

The successful raid elicited an enormous public response, including celebrations in the streets of American cities. But the operation also highlighted limitations and downsides of this type of counterterrorist use of military force. The US president ordered the raid even though the available information was far from conclusive as to whether bin Laden would be found at the compound. Questions were quickly raised after the raid about the need to kill bin Laden; the United States said that its forces were prepared to capture him but that resistance made the killing necessary.

The biggest problems involved a rapid worsening in US relations with Pakistan, where many people considered the raid a violation of sovereignty and where the Pakistani military – which had not been informed in advance – was deeply embarrassed by the operation. The location of bin Laden's hideout in central Pakistan, close to a Pakistani military academy, stoked suspicion in the West that he had received official help in staying hidden.

Debate also ensued about how much damage the killing of bin Laden inflicted on terrorist capabilities. Material seized during the raid confirmed that bin Laden's role in his last few years had been confined mostly to exhortation, not command and control. His personal following and skill as a propagandist nonetheless meant that his death was probably a significant loss to al-Qa'ida, one that cannot be fully replaced by his less charismatic successor, Ayman al-Zawahiri.

Most citizens never experience directly anything having to do with the controversial procedures just mentioned. But they do experience other conflicts between counterterrorism and important public values. There is unavoidable conflict with two values in particular: liberty (absence of restrictions on daily life) and privacy (avoiding governmental scrutiny of personal matters). Liberty is curtailed every time one is denied access to a formerly public place in the interest of security, or one has to empty pockets and detour through a metal detector to enter a building. Privacy is compromised when government agencies collect and exploit financial, travel, or other data on individuals in the interest of identifying possible terrorists. Issues of privacy became especially acute in the United States with the expansion of investigative activities after the 9/11 attacks. Debate centred on, for example, the Federal Bureau of Investigation's new power to require public libraries to identify which books an individual had borrowed, or the National Security Agency's interception of telephone conversations without a court warrant. The controversies eased somewhat with new legislative restrictions on communications intercepts and shifts in policy from Bush's administration to that of Barack Obama (Lynch 2010), but the underlying conflicts among social and security objectives remain.

There is no single, optimum formula for resolving these conflicts. Counterterrorism is not the only objective in public policy, nor should it be.

It is up to each country's citizenry, preferably acting through a fair process of representative government, to decide where it wishes to strike a balance between safety from terrorism and other interests and values.

A citizenry's confidence that this balance has been struck properly and in a way consistent with its values is important for the final, critical ingredient in counterterrorism: informed and sustained public support. That type of support is difficult to get. Public interest in counterterrorism is high after a major terrorist attack, but tends to wane if time passes without more such attacks. A counterterrorist programme can be effective only if government officials and private citizens alike understand that the programme must be applied consistently, coherently, and over a long time.

Further reading

Gabriella Blum and Philip B. Heymann, *Laws, Outlaws, and Terrorists: Lessons from the War on Terrorism* (MIT Press, 2010). Examines the legal, ethical, and practical dimensions of some of the most controversial recent issues in counterterrorism.

Daniel Byman, *The Five Front War: The Better Way to Fight Global Jihad* (John Wiley and Sons, 2008). Offers a general strategy of counterterrorism.

Audrey Kurth Cronin and James M. Ludes (eds.), *Attacking Terrorism: Elements of a Grand Strategy* (Georgetown University Press, 2004). Surveys the principal counterterrorist instruments and some of the major considerations that arise in using them.

Paul R. Pillar, *Terrorism and U.S. Foreign Policy* (Brookings Institution Press, 2003). A general treatise on counterterrorism that also places the subject in a broader policy context, with particular reference to the United States.

Richard A. Posner, *Preventing Surprise Attacks: Intelligence Reform in the Wake of 9/11* (Rowman & Littlefield, 2005). Analyses the challenges of applying intelligence to counterterrorism.