Technology, strategy and counterterrorism

PAUL CORNISH*

The terrorist attacks in New York and Washington on 11 September 2001 (9/11) represent a watershed in post-Cold War strategic thinking. There had, of course, been plenty of terrorism before September 2001; in the United Kingdom, for example, terrorism had been a serious national security concern since the late 1960s. There had also been plenty of strategic thinking for the ten years or so following the end of the Cold War in 1989–90. But 9/11 altered the general perception of terrorism and had a radical effect on security policy and strategy. In the first place, 9/11 showed that terrorism could have an impact on a scale that no previous terrorist attacks had been able to achieve. Second, the attacks showed that terrorists could use sophisticated technology (passenger aircraft) in a simple and brutally effective way (as fuel-laden guided missiles) against vulnerable, indefensible yet highly significant targets (the World Trade Center and the Pentagon) in a country generally acknowledged for its technological supremacy, indeed presumed invincibility (the United States). The effect on security policy and strategy was immediate and powerful. As the twenty-first century began, international terrorism, rather than figuring merely as one among a range of strategic challenges with which governments would have to contend—international crime, narcotics trafficking, piracy, weapons proliferation, humanitarian intervention and so on—became the focus of strategic thought and policy. And, as this article will suggest, much of that strategic attention was to be turned on technology, as a component both of the terrorist challenge and of governments' response.

For some, 9/11 was evidence that international terrorism had become a *fundamental* (rather than merely *radical*, and least of all simply *technological*) challenge to western society and values. In what was to become a long-running and vigorous debate, the conservative columnist and essayist Charles Krauthammer later insisted that 'September 11 reminded us rudely that history had not ended, and we found ourselves in a new existential struggle, this time with an enemy even more fanatical, fatalistic and indeed undeterrable than in the past'.[1] In a similar vein, and at about the same time, Britain's Prime Minister Tony Blair argued that

* I am grateful to Stuart Croft, Andrew Dorman, Anthony King and one anonymous reviewer for their comments on an earlier draft of this article.

[1] Charles Krauthammer, 'In defense of democratic realism', *The National Interest* 77, Fall 2004, p. 15.

International Affairs **86**: 4 (2010) 875–888

'the nature of the global threat we face in Britain and round the world is real and existential'.[2] In the immediate aftermath of 9/11, however, the posture adopted by Blair's government was instead to offer a more measured demonstration of solidarity with the United States, its principal ally, and an acknowledgement that terrorism had now become a more significant national security challenge. In a July 2002 defence policy paper, in which the attacks were condemned as 'unprovoked' and 'shocking', the Secretary of State for Defence noted that '11 September and its aftermath underlined the importance of the transatlantic relationship. From the outset we demonstrated by our actions our wish to work closely with our most important ally, the US.' The document also observed that terrorist action of the sort seen on 9/11 could have 'the *potential* for strategic effect'.[3]

Three years later, Britain had its own experience of suicidal terrorism and the tempo of UK counterterrorism policy increased dramatically. On 7 July 2005, in a coordinated attack on London's public transport system, four suicide bombers killed 52 passengers and injured as many as 700 others. Two weeks later, the public transport system was again disrupted by a coordinated attack by four terrorists, although on this occasion their suicide bombs failed to explode. The July 2005 attacks provoked Britain's government, security and intelligence agencies and police service into a surge of activity which has been maintained ever since. Yet at first the British government chose to maintain its rather phlegmatic approach to the terrorist challenge. The first edition of the UK National Security Strategy, published in March 2008, acknowledged that terrorism 'represents a threat to all our communities, and an attack on our values and our way of life', but insisted that terrorism 'does not at present amount to a strategic threat'.[4] Within 15 months, however, international terrorism had been elevated to a strategic-level concern: the 2009 version of the National Security Strategy describes the threat from international terrorism as 'severe' and a 'constant and direct threat to the UK and our people'. Al-Qaeda and its affiliate organizations are described unequivocally as 'the pre-eminent threat to the UK and our allies'.[5]

As terrorism took the central place in the strategic debate in the UK and elsewhere, and as the technological dimensions of both terrorism and counterterrorism became more apparent, so the long-established relationship between technology and strategy was brought to mind. If strategy is society's use of its armed forces and other resources for political ends such as protecting territory and interests and defeating adversaries, then an important part of national strategy has always been technology. Buzan has summarized the traditional technological–strategic relationship succinctly in the following way: 'Technology is a major

[2] Tony Blair, speech in his Sedgefield constituency, 5 March 2004, http://guardian.co.uk/politics/2004/mar/05/iraq.iraq/print, accessed 19 May 2010.

[3] Ministry of Defence, *The Strategic Defence Review: a new chapter*, vol. 1, Cm. 5566 (London: HMSO, July 2002), pp. 4–7 (emphasis added).

[4] Cabinet Office, *The National Security Strategy of the United Kingdom: security in an interdependent world*, Cm. 7291 (London: TSO, March 2008), p. 11.

[5] Cabinet Office, *The National Security Strategy of the United Kingdom: Update 2009. Security for the next generation*, Cm. 7590 (London: TSO, June 2009), pp. 6, 11.

International Affairs 86: 4, 2010

factor in determining the scope of military options, the character of military threats, and the consequences of resorting to the use of military force.'[6]

The purpose of this article is to enquire into the nature of the technological–strategic relationship upon which governments, including that of the UK, must draw as they confront the challenge of international terrorism. To what extent will the historical idea remain relevant and useful, and where will new thinking be required? The article begins with a summary of the historical relationship between technology and strategy generally, before describing the evolution of the British government's position concerning the more specific relationship between technology and counterterrorism. The third section of the article asks whether a traditional understanding of the technological–strategic relationship can keep pace with the new challenges of terrorism and questions certain of the ideas which appear to have informed the UK's position on the role of technology in counterterrorism.

Technology and strategy: a sketch

A standard account of the relationship between technology and strategy might describe it in several categories, the first of which would include a series of innovations (usually concerning weapons) which have proved to be tactically decisive (i.e. battle-winning). The expectation that military innovation will confer a decisive advantage in battle has been a particular feature of industrialized warfare, reflected in the words of Hilaire Belloc's entrepreneurial anti-hero William Blood. When faced with a mutiny on an expedition to Africa, Blood infamously remarks: 'Whatever happens, we have got the Maxim gun, and they have not.'[7] But the development and application of decisive weapons long predates the Industrial Revolution, of course, and has taken a variety of paths. Military history records weapon developments which have been remarkably simple, as well as others which have been remarkably sophisticated. Some have been achieved in a singular moment of invention while others have evolved through incremental improvement. The list of decisive battlefield weapons would be lengthy and would almost certainly include the crossbow, the longbow and the bayonet, as well as a series of developments in firearms: the flintlock, the breech-loader, the rifled bore, the pistol, the machine gun and so forth.

The second category would take account of tactically decisive developments which have nothing directly to do with weaponry but have acted as a 'force multiplier' in battle: the stirrup, camouflage and battlefield radio communications come readily to mind. A third category would include those moments at which innovation has had a decisive effect at the strategic level (that is, the level at which the outcome of war itself is shaped, rather than battles won): radar; the long-range bomber aircraft; the submarine; and the Colossus code-breaking

[6] Barry Buzan, *An introduction to strategic studies: military technology and international relations* (London: Macmillan, 1987), pp. 6–7.

[7] Hilaire Belloc, *The modern traveller* (London: Edward Arnold, 1989), p. 41.

International Affairs 86: 4, 2010

computers used by the British to decrypt German signal traffic during the Second World War. A fourth and final category would encompass innovations which have had a paradigm-shifting or metastrategic effect in that they have altered the very nature of war. The development and use of the atomic bomb in the 1940s serves as the most obvious example of innovation on this level. More recently, some have argued that warfare has been transformed fundamentally by developments in information and communications technology—a phenomenon known since the early 1990s, in the United States and elsewhere, as the 'revolution in military affairs'.[8]

It is not simply the material products of the relationship between technology and strategy that have been of interest, but also the changing dynamics of that relationship as well as its broader patterns and implications. It is useful to think of the technology–strategy relationship as having metamorphosed through several stages. Thus, the industrial age is generally considered to have had a considerable effect on the technology–strategy relationship, enabling technology to become more influential than ever before. In *The social history of the machine gun* John Ellis describes the American Civil War as 'the first example of an industrialised conflict, in which technological advances dictated *much of the actual conduct of the war*'.[9] Michael Howard observes a broader social effect arising from the same phenomenon: an effect which would change the style of warfare fundamentally, endowing it with certain characteristics with which the twentieth century was to become all too familiar. Nineteenth-century industrial mass production of weaponry, argues Howard, with such innovations as finely machined and interchangeable weapon parts, made 'mass participation in warfare both possible and necessary'.[10]

By the end of the Second World War the technology–strategy relationship was on the verge of another shift. Historically, as we have seen, military technological developments have had a decisive effect on warfare and have even influenced the character of war itself. But the hierarchy in this relationship was always clear: technology (no matter how innovative or decisive) served the higher politics of national strategy, and not vice versa. National strategy was not something to be determined by technology, and was in any case too complex and refined to be understood by mere technologists, engineers and inventors. The Second World War brought about a blurring of these boundaries and altered the dynamic of the relationship. In the case of the United Kingdom, and the military planners who sought to reorganize a national strategy in the aftermath of that war, the military technology seen during the conflict—air and rocket attacks, the use of submarines

[8] See e.g. D. Jablonsky, *The Owl of Minerva flies at twilight: doctrinal change and continuity and the revolution in military affairs* (Carlisle Barracks, PA: US Army War College, Strategic Studies Institute, May 1994); M. J. Mazarr, *The revolution in military affairs: a framework for defense planning* (Carlisle Barracks, PA: US Army War College, Strategic Studies Institute, June 1994); and, for a broader view, C. Gray, *Modern strategy* (Oxford: Oxford University Press, 1999), pp. 200–205, 243–54.

[9] John Ellis, *The social history of the machine gun* (Baltimore, MD: Johns Hopkins University Press, 1975), p. 47 (emphasis added).

[10] Michael Howard, *War in European history* (Oxford: Oxford University Press, 1976), p. 120.

International Affairs 86: 4, 2010

and, of course, the atomic bomb—had left an impression. This impression was so deep that the military chiefs of staff agreed that technology should be understood as a dynamic driver of strategy which must be kept under constant review; and, furthermore, that the principles of defence policy could no longer determine technological developments; the two must now interact.[11]

The second half of the twentieth century saw further developments in the technology–strategy relationship, with the most far-reaching implications for policy and strategy and for the very idea of war. No longer the *subordinate* to strategy it had been for so long, technology also escaped the bounds of the *partnership* with strategy envisaged by the British chiefs of staff to become the *determinant* of strategy. With the advent of atomic, nuclear and thermonuclear weaponry, with intercontinental-range ballistic missiles capable of ever-increasing accuracy, and with dramatic progress in communications and computing technology, war between the most technologically advanced states (or the threat of it) promised unprecedented and unimaginable levels of destruction. In Ellis's view, technology was beginning to have a 'dehumanizing' effect on war: 'On the conventional battlefield men are increasingly being replaced by electronic devices … Men are merely helpless bystanders. With the advent of nuclear weapons this process has been carried to its logical conclusion … Nuclear weapons are controlled by unimaginably complex electronic systems.'[12] These 'unimaginably complex systems' were, of course, managed (or at least monitored) by human beings, albeit far removed from the battlefield. Nevertheless a nuclear conflict, as envisaged during the Cold War, would have less to do with organized armies deployed in the field as technology placed 'increasing power in the hands of highly qualified technicians'.[13] David Edgerton makes a similar point: 'The atomic bomb, the great glory of civilian academic science … led to a new kind of war or non-war directed by civilian Dr Strangeloves.'[14]

In the final stage of the metamorphosis, occurring in the late twentieth and early twenty-first centuries, technology might have broken free altogether from its relationship with strategy. Buzan refers to the 'relentlessly expanding human knowledge that drives the technological imperative'.[15] If the task of strategy is to ensure the security of states, the challenge, in Buzan's words, is 'to adjust military strategy to meet that end in an environment dominated by continuous and often quite radical technological and political change'.[16] But the pace of technological change is now such that strategy can barely keep up, with the result that it becomes ever more difficult to organize and rationalize fast-evolving technology within some kind of strategic or security policy framework. Technology has also acquired its own momentum; there is no longer any need for a national strategic stimulus to, or context for, technological innovation which is now as likely, if not

[11] Paul Cornish, *British military planning for the defence of Germany, 1945–50* (London: Macmillan, 1996), p. 105.
[12] Ellis, *The social history of the machine gun*, p. 180.
[13] Howard, *War in European history*, p. 120.
[14] David Edgerton, *The shock of the old: technology and global history since 1900* (London: Profile, 2008), p. 140.
[15] Buzan, *An introduction to strategic studies*, p. 290.
[16] Buzan, *An introduction to strategic studies*, p. 289.

International Affairs 86: 4, 2010

more likely, to be a response to commercial opportunity or international demand as to national security.

The image which best summarizes the contemporary relationship between technology and strategy, therefore, should be that of technology racing ahead and national strategy struggling to catch up. And as the relationship is loosened in this way, it ought not to be assumed that in the race to catch up with technology—even if only periodically—governments will always be first.

Technology and strategy in UK counterterrorism

The UK government's response to the events of September 2001 was to produce, 18 months later, a 'comprehensive strategy … to counter the threat to this country and our interests overseas from international terrorism'.[17] The UK strategy, known as CONTEST (an apt compression of 'COuNterTErrorism STrategy') has undergone one major revision since 2003 and has acquired a good reputation internationally.[18] In parallel with CONTEST, and to a considerable degree driven by it, the UK government has also published papers concerning the role of science and technology. Taken together, these two sets of documents set out the UK government's assessment of the technology–strategy relationship in the context of counterterrorism.

The first edition of CONTEST in 2003 was concerned to a large extent with coordinating a cross-governmental response to international terrorism. The document was highly classified and was not as a whole made publicly available. What did become public knowledge was that the strategy comprises four strands or 'workstreams', known as the 'four Ps'—originally in the order 'Prevent', 'Pursue', 'Protect' and 'Prepare'. Each strand has a distinct purpose: the goal of 'Prevent' is to address the radicalization of individuals; 'Pursue' is intended to take action against terrorists and disrupt their operations, both domestically in the United Kingdom and internationally through cooperative efforts; the purpose of 'Protect' is to improve border security and reduce the vulnerability of the critical national infrastructure; and 'Prepare' is designed to ensure that the consequences of a terrorist attack can be managed. In July 2006, one year after the 2005 attacks in London and just weeks before arrests were made in connection with the 'airline plot', an open version of CONTEST was released, from which the classified elements had been removed. Although CONTEST 2006 had little to say directly about terrorists' use of technology, it did offer some indications as to the trajectory of government thinking about the role of technology in countering the

[17] HM Government, *Pursue, Prevent, Protect, Prepare: the United Kingdom's strategy for countering international terrorism* [corrected], Cm. 7547 (London: TSO, March 2009), p. 8.

[18] The EU Counterterrorism Strategy, published in December 2005, was built around four pillars not dissimilar from those in CONTEST: 'Prevent', 'Protect', 'Pursue' and 'Respond'. See Council of the European Union, 14469/4/05, REV 4 (Brussels, Nov. 2005), http://register.consilium.europa.eu/pdf/en/05/st14/st14469-re04.en05.pdf, accessed 19 May 2010. Several national governments have also taken a close interest in aspects of CONTEST and its development, including Belgium, the Netherlands, Australia, the United States and others in Europe and the Middle East.

International Affairs 86: 4, 2010

terrorist threat. From the outset, technology clearly played a significant part in CONTEST: in the 'Protect' strand there were important developments in border security (including a new e-Borders programme), in the use of biometric data and in screening technologies to improve the security of the transport infrastructure; and in the 'Prepare' strand there was a pressing interest in technology associated with the management and decontamination of a chemical, biological, radiological or nuclear (CBRN) terrorist attack. More significant, however, at least for the purposes of this article, was the acknowledgement that adaptability, agility and responsiveness would be necessary: efforts to protect the critical national infrastructure would need to keep 'in step with terrorist methodologies' and where the transport infrastructure was concerned it would be necessary to 'continually update' the work being undertaken with industry and others, 'taking advantage of new technologies, exploring applicability in new areas, and developing methods that can be rolled out in response to enhanced threat'.[19]

Intriguingly, in the revised version of CONTEST published in March 2009, the running order of the 'four Ps' was altered to 'Pursue', 'Prevent', 'Protect', 'Prepare'. This document is altogether more explicit regarding the role and significance of technology, both in the terrorist threat and in the counterterrorist response. Technology is described as one of the four 'strategic factors' leading to the emergence of contemporary international terrorist networks, offering advantages to terrorists in terms of communications and tactics.[20] The document sets out a range of planning assumptions to cover the three years to 2012. With terrorists able to exploit emerging technology in communications, surveillance, reconnaissance and weapon lethality, one of the assumptions amounted to a stark assessment of the place of technology in terrorism: 'Terrorist organisations will have access to more lethal technology. Scientific training and expertise will have even greater significance for terrorist organisations because technology will be able to compensate for the vulnerabilities they will have. Terrorists will continue to aspire to develop or steal and then use [CBRN] weapons.'[21]

As far as the counterterrorist strategy is concerned, the revised CONTEST offers a more developed discussion of the role of technology. Government will need to be more open with non-governmental partners in industry and elsewhere—moving from 'need to know' to 'responsibility to share'—and the private sector will have 'a key role to play' in the science and technology aspects of all four CONTEST workstreams.[22] The document refers to the government's 'long track record of working with the science and technology industry across the military, security and intelligence markets', but calls for 'new thinking about the ways this engagement should be managed'.[23] Government will seek better ways to work with industry—represented by a new Security and Resilience Industry

[19] HM Government, *Countering international terrorism: the United Kingdom's strategy*, Cm. 6888 (London: TSO, July 2006), p. 24.
[20] HM Government, *Pursue, Prevent, Protect, Prepare*, pp. 40–43.
[21] HM Government, *Pursue, Prevent, Protect, Prepare*, p. 49.
[22] HM Government, *Pursue, Prevent, Protect, Prepare*, pp. 116, 131, 145.
[23] HM Government, *Pursue, Prevent, Protect, Prepare*, p. 146.

International Affairs 86: 4, 2010

Suppliers' Community (RISC)—and among other goals will seek ways to 'harness the benefit of the commercially driven ICT industry to support Government security and counterterrorism requirements and explore how industry can best help with the timely detection of suicide bombers'.

More 'new thinking' was to be expected from the Office for Security and Counterterrorism (OSCT), established in the Home Office in March 2007. Reflecting the sense that technology represents both a threat and an opportunity, the task of the OSCT would be nothing less than to ensure that the government 'has the ability to respond effectively, and with pace, to developments in technology and the terrorist threat'. Among new ideas to be considered was the possibility that government could make venture capital-style investments in order to encourage innovation for counterterrorism. Ideas such as this would be expected to give the government 'greater understanding of the innovation community, smarter influence over external innovation and better coordination of investments in innovative ideas and solutions'.[24] The first CONTEST annual report, published in March 2010, reiterates certain of these themes: the OSCT's new INSTINCT (Innovative Science and Technology in Counter Terrorism) programme, intended to seek 'novel technical solutions to address challenges identified in CONTEST', is judged to have set 'new standards for industry and Government joint work on counter terrorism related issues'; while in the field of CBRN and explosives detection the document reports an 'awareness-raising programme' being developed for the 'academic sector'.[25]

In a second set of papers the UK government addresses more directly the role of technology in its counterterrorism strategy. In the *United Kingdom Security and Counterterrorism Science and Innovation Strategy*, published in 2007, the then Home Secretary Dr John Reid insisted on the need 'to develop a dynamic, innovative and integrated response to a threat which is seamless in nature'. Reid described the relationship between science and innovation technology and national security in familiar terms (science and innovation are of 'critical importance' in strengthening the UK's ability 'to combat the threat from terrorism') and noted with confidence that the United Kingdom 'has an exceptional record in delivering cutting-edge science and innovation'. In Reid's view, the distinctive feature of terrorism is that it is complex and 'ever-changing', requiring more coherence and flexibility in 'delivering and exploiting counterterrorism research'.[26] The document later refers to the need to have 'the capacity to harness science and innovation in more agile and decisive ways' in order to 'deliver science and innovation at a pace that outstrips our adversaries'.[27]

The March 2009 Science and Technology Strategy for Countering International Terrorism revisited several of these themes: international terrorism is

[24] HM Government, *Pursue, Prevent, Protect, Prepare*, p. 147.
[25] HM Government, *The United Kingdom's Strategy for Countering International Terrorism: Annual Report 2010*, Cm. 7833 (London: TSO, March 2010), pp. 17, 23.
[26] HM Government, *UK Security and Counterterrorism Science and Innovation Strategy* (London: Office for Security and Counterterrorism, 2007), foreword, p. 2.
[27] HM Government, *UK Security and Counterterrorism Science and Innovation Strategy*, p. 15.

International Affairs 86: 4, 2010

seen as a rapidly evolving threat; science and technology 'have a key part to play in our counter terrorist work'; and the United Kingdom is considered 'already a centre of excellence in innovative security technology'.[28] The document considers terrorists to have sufficient access to technology to be able to increase the lethality of their operations and challenge the security of the UK. And since science, technology and innovation are not static, terrorists will also be able to exploit advances in technology to their own ends:

> In the future, terrorists are very likely to have more scope to communicate with each other, sometimes with less chance of detection. Online communications will continue to enable extremist messages to reach vulnerable individuals faster than conventional media. Technology may provide improved surveillance and reconnaissance capability as well as more lethal weapons. Scientific training and expertise will itself have even greater significance for terrorist (and insurgent) organisations because technology will be able to compensate for the vulnerabilities they have.[29]

The 2009 Science and Technology Strategy gives the Joint Terrorism Analysis Centre responsibility for considering 'the current and future technological capabilities of terrorist organisations',[30] and is unequivocal regarding the importance of technology to counterterrorism: 'Success in delivering relevant science, innovation and technology is vital to the delivery of CONTEST. Science and technology impacts every area of the strategy. Our continued ability to identify and convict people engaged in terrorism, prevent radicalisation, protect our infrastructure and prepare for an attack all depends on developments in the physical and social sciences.'[31]

The two science and innovation/technology strategy papers, together with the series of CONTEST documents and reports, go some way to describing the UK government's position concerning the role of technology in counterterrorism. The assumptions which underpin this position will be examined below, but it is interesting to note that whereas it was suggested in the first part of the article that technology might have 'broken free from its relationship with strategy', the dominant assumption within UK government appears to be that technology—and indeed science itself—can still be enlisted in the cause of a national counterterrorism strategy.

Old assumptions: new challenges

The first section of this article presented a standard account of the relationship between technology and strategy in four categories: tactically decisive innovations in weaponry; tactically decisive innovation in military equipment other than weapons; strategically decisive innovation; and finally innovation which

[28] HM Government, *The United Kingdom's Science and Technology Strategy for Countering International Terrorism* (London: Home Office, Aug. 2009), p. 4.
[29] HM Government, *The United Kingdom's Science and Technology Strategy*, pp. 8–9.
[30] HM Government, *The United Kingdom's Science and Technology Strategy*, p. 15.
[31] HM Government, *The United Kingdom's Science and Technology Strategy*, p. 9.

International Affairs 86: 4, 2010

alters the very character of war and strategy. The question now is whether the traditional technology–strategy paradigm, as described, can meet the new and evolving challenges of international terrorism. Consequently, it must also be asked whether the United Kingdom's counterterrorism strategy seeks to meet these new challenges with assumptions about the technology–strategy relationship which are no longer applicable.

Technological innovation and inventiveness, particularly in the military area, can be stimulated by 'profound economic and social changes'.[32] Terrorists can also experience profound social and economic change, and might also be expected to be inventive. This prompts two obvious qualifications to the technology–strategy paradigm as traditionally understood: not only might the adversary be capable of innovation (and perhaps even decisively so), but the adversary in this case is not a state and ought not to be expected to behave like one. How then does a terrorist behave? Do terrorists see conflict in terms of tactics and strategy? And how innovative do terrorists need to be? It is at this point that several of the categories mentioned above begin to consolidate into a larger and rather messier problem for government strategists: for terrorists, battle-winning, tactical weaponry and equipment might be little different in their effect from war-winning, strategic technology. Relatively commonplace technology (whether in general non-military use, such as ammonium nitrate fertilizer, or a military weapon such as a sniper rifle) can offer the strategic effect which the terrorist needs: as Amitav Mallik notes, 'even moderate levels of technological capability in the wrong hands will have serious security implications'.[33] Technology of this sort might not give terrorists victory, but it might prevent defeat and allow the struggle to continue, which for terrorists can be a victory of sorts. Perhaps at this level terrorists might best be understood as taking a more pragmatic approach to technology and its significance for tactics and/or strategy. Whereas for industrialized economies technology has often been regarded as an end in itself, giving rise to the notion that battles and even wars can be won through innovation and invention, for terrorists technology might be a means to an end: technology need not promise decisiveness at any level, it simply needs to be good enough to allow an attack to be made, and to be made again.

This is not to say, of course, that terrorists are not capable of innovation and ingenuity, as Bruce Hoffman's account of the evolution of IRA bomb-making makes clear.[34] Furthermore, when terrorists do innovate they can present a low–high span of inventiveness which governments might find hard to match—particularly those governments which for decades have assumed the technology–strategy relationship to be a matter of constant striving for ever more sophisticated and decisive innovation, as well as something within the scope of their own control. As Erin Gibbs van Brunschot and Leslie Kennedy observe, technological advances 'that are often outside the realm of state control facilitate the extent and reach of

[32] Ellis, *The social history of the machine gun*, p. 170.
[33] Amitav Mallik, *Technology and security in the 21st century: a demand-side perspective*, SIPRI research report 20 (Oxford: Oxford University Press/Stockholm International Peace Research Institute, 2004), p. 122.
[34] Bruce Hoffman, *Inside terrorism*, 2nd rev. edn (New York: Columbia University Press, 2006), pp. 252–4.

International Affairs 86: 4, 2010

terrorist threat. Individuals, for example, can produce knowledge-based weaponry in the privacy of their own facilities.'[35] On the one hand, terrorists can make use of relatively low-level technology, in small quantities, to achieve disproportionate effect: suicide attackers and car bombers are two cases in point. At the other extreme it is widely understood that terrorist groups are able to exploit cyberspace to great effect and are keen to acquire and use sophisticated CBRN weapons.[36] The asymmetry here is clear enough: not only must a national counterterrorist strategy be able to respond and innovate across a broader spectrum than terrorists require to be successful, it must also do so as rapidly as, if not more rapidly than, terrorists.

With respect to technology and innovation, the terrorist/counterterrorist asymmetry might represent a fundamental misalignment in approach which even the most sophisticated and responsive national strategy will be unable to correct to its own advantage. To borrow an idea from David Edgerton, it might be that terrorists have more of a 'use-based' approach to technology than an 'innovation-based' approach. 'In use-centred history,' writes Edgerton, 'technologies do not only appear, they also disappear and reappear, and mix and match across the centuries.' The use-based approach can encompass the widest variety of users, including 'all places that use technology, not just the small number of places where innovation is concentrated', and, most damagingly of all, 'undermines the assumption that national innovation determines national success'.[37] For terrorists, whether technology is simple or sophisticated, it is essentially just a commodity; a means to an end. For national governments, on the other hand, technology is too often the end in itself—as if the most sophisticated innovation conferred some sort of evolutionary advantage on those societies able to produce and control it. Ellis notes that some Europeans believed they had superior weapons (such as the machine gun) because they were 'the superior race'.[38]

Something of this hubris emerges in the UK's counterterrorism strategy and in its expectations of technology and innovation. Even though some terrorists are known to be technologically astute, there is a hint of indignation that an advanced, high-technology economy such as the United Kingdom could be wrong-footed by comparative technological primitives. There is also the enduring conviction that science, technology and innovation will offer what industrialization did in the past—a massive and overwhelming advantage in the struggle against the country's adversaries. Thus, according to the 2007 Science and Innovation Strategy, although the terrorist threat 'is ever-changing … innovative and … inventive', by exploiting its research capacity the UK can 'stay well ahead of the terrorists'. 'Hazardous threats', the document argues, 'are not new to the UK. A key way in which we have countered these threats over the years is through

[35] Erin Gibbs van Brunschot and Leslie W. Kennedy, *Risk balance and security* (London: Sage, 2008), p. 93.
[36] Paul Cornish, *The CBRN system: assessing the threat of terrorist use of chemical, biological, radiological and nuclear weapons in the United Kingdom* (London: Chatham House, 2007); Paul Cornish, Rex Hughes and David Livingstone, *Cyberspace and the national security of the United Kingdom: threats and responses* (London: Chatham House, 2009).
[37] Edgerton, *The shock of the old*, pp. xii–xv.
[38] Ellis, *The social history of the machine gun*, p. 81.

International Affairs 86: 4, 2010

science, by engaging some of the most brilliant minds in the country to create world-class knowledge to combat the threat.'[39]

Elsewhere the CONTEST and science and innovation/technology documents use language which may indicate an outdated understanding of the technology–strategy relationship. The preferred pattern for cooperation with bodies outside government is firmly centralist: it is government which possesses the critical knowledge, and it is government's task to share aspects of that knowledge with industry and others with whom it wishes to 'work closely'. This is not entirely unreasonable; relations with industry and non-governmental bodies must be governed to some extent by the highly classified nature of government work. Yet while it is clear that government must have authoritative knowledge in some areas, it would not be reasonable for government to assume authority in all areas. There are commercial companies, such as Microsoft and Google, which might consider themselves equal to any government in their understanding of the misuse of cyberspace, for example. The centralist approach to the technology–strategy relationship also presents the image of government as the controlling force. Where agility, responsiveness and 'pace' are required to deal with technologically capable terrorists, the assumption appears to be that governments are best placed to orchestrate such a response. Yet liberal democratic societies and their governments have not always demonstrated the capacity and the will to respond spontaneously and decisively to security challenges, particularly of a novel kind. Furthermore, some in the commercial sector might question whether it is indeed government's role to 'manage', 'exploit' and 'harness' new technology and exert 'smarter influence' over innovative companies and individuals which operate in the free market.

In the past it has not been uncommon for industry—particularly in the security and defence sectors—to be regarded as a strategic asset ready to be coopted into the national effort at times of emergency. The UK government's counterterrorism strategy appears to sustain that notion, and perhaps makes the even larger assumption that science itself can somehow be conscripted into national service. Yet while there is no reason to suppose that scientists, industrialists and innovators are any more or less patriotic and dutiful than other inhabitants of the United Kingdom, their motives might not always be consistent with the government's counterterrorist strategy. Although government is an important sponsor of scientific research and development, there are nevertheless scientists and technologists for whom government-sponsored research would compromise the independence and impartiality of their work. Whereas conflicts such as the Second World War were of such a scale that individuals and organizations might willingly participate in an effort of national survival, it cannot be assumed that the threat of terrorism will have a similarly unifying effect. Some will simply not share the government's assessment of national and international security and might be unwilling to become involved in efforts to 'combat' terrorism. Foreign companies based in the UK and operating in the UK science and technology sector might have their

[39] HM Government, *UK Security and Counterterrorism Science and Innovation Strategy*, p. 5.

International Affairs 86: 4, 2010

own affiliations and loyalties to consider in times of emergency. Wherever they are registered, commercial companies measure their success in terms of profit and shareholder satisfaction, and do not usually see themselves as national security agencies in waiting. With all this in mind, there is also a risk that commercial pressures might distort the technology–strategy relationship: 'Too often the agenda for discussing the past, present and future of technology is set by the promoters of new technologies.'[40]

Conclusion

The terrorist attacks in London in July 2005 prompted a surge of activity in UK national security, in terms of refining and implementing the national counter-terrorist strategy, and in terms of defining a technological counterpart to that strategy. For as long as humankind has been both strategist and technologist, there has been a relationship of sorts between these two preoccupations. This article has suggested, however, that the technology–strategy relationship is no longer as close and mutually supportive as might in the past have been the case. Furthermore, the UK counterterrorism policy appears to draw upon certain assumptions about the technology–strategy dynamic which no longer obtain. Yet for all that, it is clearly not the case that the longstanding relationship between technology and strategy has collapsed under the strain of the terrorist threat; indeed, this brief assessment of UK government policy and practice suggests precisely the opposite. The recent experience of the UK government demonstrates, instead, that a more complex understanding of the technology–strategy relationship is emerging in the context of counterterrorism.

Technology is central to both terrorism and counterterrorism, yet each side sees technology in a different way. For the government of the United Kingdom and others in a similar situation, advanced technology has long been expected to confer a decisive advantage in battle and war; and something of this expectation can be discerned in the UK counterterrorism strategy. For terrorists, however, technology is more of a means to an end. Although an attack with a CBRN weapon would certainly be regarded as a 'propaganda coup', to the terrorist it generally matters less whether technology is basic or sophisticated than whether it can enable a successful attack to be made, generating the requisite level of media interest and public anxiety. This asymmetry in expectations is mirrored by asymmetry in the resources and effort devoted to developing and implementing technological solutions. In the UK and elsewhere the counterterrorism effort has been vast in scope, scale, technological sophistication and of course expense. Yet the terrorist does not necessarily require sophisticated technology in order to carry out an attack, and does not judge its success in technological terms.

Recent UK experience also suggests that if the technology–strategy relationship is not managed carefully there may be perverse consequences, either by giving the terrorist more importance than he deserves, or undermining important aspects

[40] Edgerton, *The shock of the old*, p. ix.

of society's resilience to terrorism. Although expert in asymmetric conflict, the terrorist cannot hope that some technology or other will enable him to *seize* victory from his technologically, militarily and economically superior adversary. The most the terrorist can hope is to be *granted* victory, slowly and incrementally, by his opponent. The terrorist's ideal adversary is a government which either uses technology disproportionately in response to the terrorist threat or defines its struggle against terrorism in narrowly technological terms and in so doing presents its more or less technologically competent adversary as its strategic equal. From the perspective of government and society, technology cannot eliminate all risks and threats and guarantee an impenetrable defence, nor can it guarantee to defeat terrorism. Instead, the most that can be expected is that technology be used to increase the costs of terrorist activity to the point where even incremental victory is perceived to be unlikely and the terrorist effort begins to lose its energy. But if the aim is to induce entropy in the terrorist's campaign, then society's resilience to terrorist threats and attacks is just as important as the proportionate use of technology.

One distinctive characteristic of the technology–strategy dynamic in counterterrorism is that this otherwise rather arcane relationship is observed and experienced in an unprecedentedly public way, such that Michael Howard's 'mass participation' now refers not simply to massed armies but to society as a whole. Counterterrorism strategy might make a strong case, either generally or at specific moments, for the use of identity checks, body scanners, CCTV and other sophisticated security technologies. But the vast majority of the individuals, groups and organizations experiencing these security measures will have little familiarity with the purposes and imperatives of counterterrorism strategy, and their tolerance of its intrusions amounts to a new determinant of the success or otherwise of the technology–strategy relationship. Public tolerance will be shaped by arguments about civil liberties and by suspicion of a 'surveillance society', and more prosaically by irritation at the inconvenience and delay caused by security checks and so forth. Yet whatever its source, and however intractable and inconvenient, it is this public tolerance of security technology which most closely represents normality, the resilience that is society's strongest defence against the threat of terrorism. At one level, therefore, the challenge to government is to maintain a technological edge against its terrorist adversary, without exaggerating the adversary's capability. But the greater challenge is to ensure that the technology–strategy relationship does not become unbalanced, with technology regarded somehow as an agency in its own right, able to compensate for any paucity in strategic thinking. Resilience is key to the success of the UK's counterterrorism strategy. And strategy must be concerned, as it has always been, with the achievement of political goals. In the era of mass (that is, societal) participation in strategy, it becomes ever more important that these goals are articulated coherently and, above all, persuasively.

International Affairs 86: 4, 2010