Assume that terrorism with the destructive intent demonstrated on September 11, 2001 (9/11) will be a continuing threat, and not a one-off, and a threat is to Western capitalism as a whole, not just the United States (US). Assume also that a continuous information revolution of computers and electronic communications – referred to here simply as information technology (IT) – is really in progress and will continue, with government intelligence as an integral part of it. Should these two assumptions combine to make us think radically about intelligence? It is getting more money and attention everywhere. In the present British political idiom about public services, how is government to ensure that it delivers.

Well before 9/11 there was extensive American writing about the need for intelligence change. Some of it was about the perceived weaknesses of particular American organisations. The National Security Agency (NSA) was said to be fossilised; the new National Imagery and Mapping Agency (NIMA) should never have been created in the first place; the Defense Intelligence Agency had never found its real métier; the Central Intelligence Agency (CIA) to some writers was too civilian, and to others had become too oriented after the 1991 Gulf War to military support, while one or two argued that it should never have been created in the first place. The Director of Central Intelligence (DCI) at the apex of the structure was held to be ineffectual, without direct control of money and jobs. To some extent all this reflected the American national propensity for self-criticism; if anything is important enough, there must be ways of doing better.

This literature also had a strain of managerial radicalism in it, linked with the IT revolution. Information and information-handling were being transformed, and intelligence must follow suit. There was a consensus about the need for change, though less agreement on the direction. Robert Steele argued for re-thinking intelligence as a whole, putting far more emphasis on open sources and cooperation with non-governmental sources of information; a change in boundaries was needed ‘away from a small group of secret government bureaucracies and toward a larger conception of a
“virtual intelligence community” that harnesses the distributed intelligence of each nation, creating “smart nations”...Bureaucracies are bad. Secret bureaucracies are worse.”

Others believed that, even if intelligence’s boundaries remained unchanged, something drastic had to be done to its internal structure. Bruce Berkowitz and Allan Goodman represented this school of thought in claiming in 2000 that the information revolution pointed to a new ‘decentralised, market-based, fluid model’ for intelligence, the antithesis of all the bureaucratic regularities. ‘If it is to remain effective, the intelligence community will have to change – so much, that when these changes are completed, it will likely bear little resemblance to the organization created fifty years ago.’

The 9/11 attack produced some changes. Terrorism was already a top priority but became the super-priority, and budgets have increased correspondingly. The political climate in which Western intelligence operates has altered, quite dramatically in the US and more subtly elsewhere. New overseas intelligence liaisons have become acceptable and have been developed. New legislative balances are being struck domestically between extended intelligence coverage on the one hand (and the admissibility of its evidence in legal processes), and citizens’ privacy on the other.

Most of these changes are not new in kind, and reinforce the developments of the last decade towards increased international cooperation and military intervention in an increasingly turbulent and dangerous world. But 9/11 has meant a change of national mood, which the subsequent US concentration on Iraq has intensified and not dissipated. According to President Bush’s National Security Strategy presented on 20 September 2002, ‘intelligence – and how we use it – is our first line of defense against terrorists and the threat posed by hostile states’, and despite policy differences America’s allies are following this general lead. It would be surprising if the mood has not had some influence in Russia, China and elsewhere outside the nominal Western camp. Intelligence is riding high worldwide and will continue to do so.

This has been accompanied in the US by renewed calls for intelligence reform, yet since 9/11 these have remained largely unfocused. American Congressional post-mortems have not got very far and did not secure the administration’s cooperation. The Executive and Legislature have been embroiled in action rather than reflection, and the pace of events has given most commentators too many other things to think about. British criticism of intelligence over 9/11 has been muted for similar reasons, and because it became known that the Joint Intelligence Committee (JIC) had actually warned ministers in July 2001 that plans for the Al-Qaeda attacks were in
the final stages of preparation, though the timings, precise targets and methods were not known.\textsuperscript{5} 

This lack of focus may change. President Bush has endorsed the need for intelligence reform, including better warning capabilities.\textsuperscript{6} Eventually there may be time for governments to stand back and consider lessons coolly, though at the time of writing one would not bet on it.

Be that as it may, the case for a rethink remains. Global terrorism poses many requirements, but the assumptions set out at the beginning of this article point to what may be the a central issue. If the IT revolution is a ‘given’, does it have a direct bearing on counter-terrorism? If so, does it point to applying technology in a gradual and evolving way, or to the more radical approach suggested in the pre-9/11 literature? And if the latter, in what direction? These are the questions for this article, using British and American examples to illustrate general issues for intelligence everywhere.

COUNTER-TERRORISM AND INFORMATION MANAGEMENT

Counter-terrorist intelligence is nothing new, but its importance now warrants regarding it as an intelligence discipline in its own right, with equal standing to the accepted ‘political’, ‘military’ and ‘economic’ categories of collection and product. Like these other categories it serves policy-making and decision-taking at all levels: strategic, operational and tactical. Its most important and direct value is in providing pre-emptive tactical warning of terrorist action, though even this may not result in immediately observable action such as arresting terrorists or capturing their matériel. Warnings may be effective defensively rather than offensively, as illustrated in Dame Stella Rimington’s claim in 1994 that the security forces in Northern Ireland were by then frustrating four out of every five attempted terrorist attacks, without necessarily disrupting the terrorist units involved.\textsuperscript{7} Warning may also be used defensively at the general operational level of updating the threat assessments that gear defensive security policies to the best estimates of risks and vulnerabilities. Intelligence success in the short and long terms may be simply in contriving that nothing happens.

Nevertheless counter-terrorism in most of its applications operates characteristically on twin tracks of timeliness: on one track the long-term research and source development characteristic of ‘difficult’ targets, and speedy reaction on the other track. It combines the patience of counterespionage’s detective work and counterintelligence’s penetration of the adversary with the agility of military intelligence’s wartime tactical applications and the ‘quick response’ aspects of law enforcement. It needs a
scholarly attention to detail and objectivity, yet the destructiveness of 9/11 emphasised the intensity with which it has to work; tactical warning must be given in time. In this respect counter-terrorist intelligence comes close to counter-terrorist action, and the two are sometimes almost indistinguishable; yet they need to be considered separately. ‘Counter-terrorism’ is used here for convenience, but relates throughout to intelligence and not action taken on it.

As such, counter-terrorism’s tradecraft embodies the central importance of secret sources; the identifying and tracking of people (rather than the military accent on equipment, for example); and, now, a combination of specific expertise on difficult languages and terrorist culture with a more general global-mindedness. Terrorism’s global disposition and reach requires a comparably global counter-terrorist reaction. The merging of ‘domestic’ and ‘foreign’ intelligence is even more complete now than in earlier, more geographically constrained campaigns such as those against the IRA.

Most of these features are reflected in a notable current account written by a member of the British Security Service’s International Counter Terrorist Branch. He argues that counter-terrorist intelligence is neither a chess game against a single enemy, nor is it like completing a jigsaw puzzle, unless it is accepted that the picture is fragmentary and fleeting with many pieces in the box that fit nowhere. For the ‘needle-in-a-haystack’ search for clues, he prefers a metaphor of tracing threads and weaving patterns. The raw material is itself variegated and extensive, including:

- secret intelligence such as the intercepted communications of known terrorists;
- secret intelligence on those, perhaps overseas, known to have been involved in terrorist support activity in the past;
- reports from overseas security organisations (again of highly variable quality and sometimes politically coloured) on actual or possible terrorist planning;
- police reports, for instance of suspicious movements through ports;
- allegations from ‘walk ins’ who claim to have inside knowledge of terrorist plans;
- calls from members of the public reporting their suspicions;
- media statements by spokesmen for terrorist groups or their sympathisers.

The quantity of material coming in is immense – and to some extent driven by market forces. If someone is willing to pay for counter-terrorist intelligence then you can be sure that someone else is willing to supply it – manufacturing it first if necessary.

On this material

the job of the intelligence officer is to identify those strands that are worth pursuing and then to pursue them until either they are resolved,
or they start to look flakey and not worth pursuing, or there is nothing more that can usefully be done. It is a risk management process. The number of potential leads that can be followed is virtually infinite. On the other hand, covert investigation is extremely resource-intensive and impinges on the human rights of the subject. The threshold for such investigations is therefore high and the number of investigations necessarily limited. Consequently many potential leads have to be discounted. Decisions on which leads to pursue are vital, but they are also complex and rich in judgement.

Some American discussion – both before and after 9/11 – has had a different focus: on improving collection, with a special emphasis on human sources. Some writers have portrayed human sources (Humint) as the answer to terrorism. Even in Britain a usually sensible MP has managed to bring a political bias into urging this need for more Humint: ‘…instead of recruiting more establishment-type Oxford and Cambridge graduates, MI6 needs recruits who will mix easily in the coffee bars of Kandahar’.9

Such sentiments have an element in them of naivety and the search for panaceas. Good human sources are of course worth their weight in gold; success in the UK’s battle against the IRA depended in large measure upon them. The American commentators may indeed have been correct in arguing that the CIA’s Directorate of Operations had become demoralised in the 1990s by persistent public and congressional criticism and lack of managerial support. But even the best Humint – and the extensive liaison with foreign services it often entails – will not provide a magical solution on targets of the Al-Qaeda kind. Hence the importance of the analogy of thread-developing and weaving, searching and making connections in many different kinds of information: secret and non-secret, domestic and foreign, with many different provenances. Counterintelligence is particularly all-source and holistic.

This makes it a ‘natural’ for advanced IT. Technology is affecting all parts of the intelligence process, from collection (and its targets’ defences against it, as through the commercial availability of encryption systems) through processing and analysis to delivery to customers. But its special relevance to counter-terrorism is probably its expanding scope for searching large swathes of data and making connections in them, in ways previously impossible: a revolution in the scope for bringing all evidence together automatically for the process of testing and developing the possible ‘threads’. There is the obvious parallel with police methods; no murder investigation in Britain would now take place without an IT system to handle the evidence. But for counter-terrorism the need is for much wider searches in databases with many different levels of IT compatibility and sophistication.
Here a current military analogy is relevant. The literature since the 1991 Gulf War on the so-called Revolution in Military Affairs (RMA) has centred on IT’s ability to develop a ‘system of systems’ to knit together the separate IT of Intelligence, Surveillance and Reconnaissance and other information sources, to provide immediate and common ‘situational awareness’ of the battlespace, a form of ‘network-centric’ warfare in which information is shared and readily available at all relevant levels of command. The suggestion here is that counter-terrorism can have its comparable IT vision: a ‘system of systems’ to make all the different kinds of relevant data accessible by every counter-terrorist analyst at every IT workstation.

Analysts would still specialise in particular targets or particular kinds of evidence, but would have a more comprehensive and immediate view of all relevant material, including ‘collateral’ from unusual sources, than has ever been possible by traditional methods, with a correspondingly increased and more timely ability to ‘thread’ and ‘weave’ connections in the evidence. Work on counter-terrorism would produce better insights, more sensitive steerage of investigation and quicker tactical warning. IT’s potential and terrorism’s threat combine to suggest this as a strategic vision. If so, how then do we get from here to there?

INSTITUTIONAL BARRIERS

The vision is of revolutionising information flows across inter-institutional boundaries. (Improved flows within organisations may be almost as important, but are not considered here.) The boundaries are of two different kinds. One is between the different organisations for collection and analysis in what is dubbed the ‘intelligence community’ – officially designated by Executive Order in the US, and corresponding with membership of the JIC in the UK. Thus the boundaries within the community between the CIA’s ‘foreign’ intelligence and the Federal Bureau of Investigation’s (FBI) ‘domestic’ intelligence appear on present showing to have been a key factor in the failure to provide warnings of 9/11. The other kind of boundary is between this intelligence community and other bodies outside it. Both kinds of boundary pose the same problem: ‘the difficulty of achieving horizontal integration in a vertically funded world’, in which vertical authority and prerogatives create tensions between immediate institutional interests and the broader common good; common interests compete with turf dominance.

Intra-Intelligence Barriers

On the intelligence community itself, American writers have extensively criticised the ‘stovepiping’ effects of the separate agencies, in which single-source intelligence is passed up to the top without sufficient all-source
integration, and without sufficient cooperation in the steerage of collection. They point to the production and marketing of single-source rather than all-source material, the prevalence of inter-agency rivalry and demarcation problems, and the difficulty of pursuing community rather than sectional interests. As an earlier example of stovepiping in the present writer’s experience, American satellite imagery in the Cold War was a technical and professional miracle, but its handling in separate organisations with separate security regulations meant that it was difficult for anyone to integrate it properly with other technical collection.

There must be some suspicion that this stovepiping has become a convenient whipping boy in the American writing for almost every kind of shortcoming. Intelligence puts a special emphasis on reliability, and organisational divisions are needed to maintain varied kinds of special expertise and establish rules of accountability. Intelligence cannot just be an all-source free-for-all. The issue is not the existence of the stovepipes but their number, their length and the arrangements for junctions with others.

Nevertheless the problem remains of vertical institutional barriers. The intelligence agencies that developed in the course of the twentieth century are remarkably powerful, autonomous and resilient. In Britain the pattern of the separate agencies, distinct from military intelligence and police forces, dates back essentially to the post-World War I reorganisation of 1919 which established the Security Service and Secret Intelligence Service (SIS), and gave Signals Intelligence (Sigint) a position of some independence under SIS’s chief; and this structure has been unaffected by the incessant reorganisation of the rest of the public sector over the past 30 years.

Something of the same relative stability has applied in the US; the creation of the NIMA has been the only major institutional innovation since the establishment of the Defense Intelligence Agency and National Reconnaissance Office in the early 1960s. Institutional separation is very deeply entrenched. After practical experience of the American intelligence community and the separate institutions within it, Gregory Treverton memorably commented on it that ‘community describes precisely what it is not: it is somewhere between a fiction and an aspiration’.13

Separate and long-standing institutions of any kind develop proprietary instincts about ‘their’ information, but in the case of intelligence these have been multiplied many times over by the secrecy needed for source protection. Intelligence in the half-century after World War II developed an ever-increasing labyrinth of special classifications and compartments, designed explicitly to control information flows; justifiably so, in the light initially of the scale of Soviet espionage and subsequently of leakages to the media, but with damage nevertheless to intelligence’s effectiveness.14
Partly for these security reasons intelligence over the same period regularised the conventions of inter-agency exchanges. Intelligence information was either included in the formally ‘published’ product which agencies sent to their ‘customers’, or remained as ‘unpublished’ material in agency files and was not available to others. Intelligence as a whole developed its philosophy of output as a service to ‘customers’ outside the community, rather than to ‘collaborators’ inside it; and IT was planned essentially on that single-agency basis, and not for community access. The community could connect separate items of published information, but it had no means of connecting individual items which did not meet publication thresholds on their own and hence lay unpublished in two, three or four different agencies, but might have been significant if put together.

There were good reasons for all these developments. But one result was the growth of some formality and rigidity in intelligence dissemination. I have written elsewhere of the ways in which the institutional boundaries between single-source and all-source analysis could impede what intellectually is really an all-embracing search for truth, ideally a jeu sans frontières.\textsuperscript{15} Something of an earlier informality of that kind can be found in R. V. Jones’ account of British scientific and technical intelligence between 1939 and 1945,\textsuperscript{16} but there was rather less place for it in the long years of peace that followed.

Extra-Intelligence Barriers

Similar considerations apply to horizontal flows between the intelligence community and bodies outside it. Counter-terrorism needs ad hoc access to some data normally quite unrelated to it: perhaps company data, driving licence applications, passenger lists and manifests as examples. (The American government research programme of Total Information Awareness envisages a matching of much more extensive personal data to trace terrorists, including \textit{inter alia}, passport and visa applications, criminal, education and housing records, travel and transportation information, as well as personal identity data like fingerprints and iris scans.)\textsuperscript{17} Much more regular contact is certainly needed with the law enforcement agencies in which specialised ‘intelligence’ is becoming a new quasi-community in its own right. In Britain this is led and coordinated by the National Criminal Intelligence Service (NCIS); in the US the connection between the intelligence community and law enforcement is encapsulated in the dual roles of the FBI, though there are many other law enforcement agencies. In both countries the secret agencies of the ‘old’ intelligence communities have increasing links with this ‘new’ law enforcement intelligence on subjects like drugs trafficking, and counter-terrorism has made these connections more important. An example is the study of terrorist funding, said to be performed
in Britain principally by the NCIS.\textsuperscript{18} Even apart from these connections between intelligence specialists, law enforcement bodies as a whole are necessarily close to terrorism, and are both prime customers for intelligence on it and contributors of the information they gather themselves. Terrorism accentuates the need for horizontal information access between these two communities; IT provides the potential for doing so.

So the IT vision of an overarching ‘system of systems’ and a counter-terrorist \textit{jeu sans frontières} really has two parts: within the intelligence community itself (let us call it the ‘Mark 1’ system), and between the community and other bodies, particularly in law enforcement (the ‘Mark 2’ equivalent). For reasons that will be apparent, this article concentrates on Mark 1, even though for counter-terrorism some aspects of Mark 2 are equally important.

\textit{Realising the Information Technology (IT) Vision}

For the intelligence community itself (the Mark 1 system) a simplistic answer would be to reorganise; to solve the problem of IT interoperability by following the modern fashion for ‘agile organisation’ and moving all those working on counter-terrorism into a new organisation geared exclusively to that target. There was some suggestion of this in the recent hearings of the British Parliament’s Defence Committee – not the Intelligence and Security Committee – and the idea has been floated by some American politicians.

It is not completely without merit. The main intelligence agencies are often seen as specialists in particular methods and material – Humint, Sigint, imagery and other smaller specialisations – yet the security services among them are in reality specialists in a subject: covert threats to internal security. It would be interesting to consider, counterfactually, whether Britain in 1969 would have been wise to create a more interdisciplinary, target-driven counter-terrorist organisation of this kind, perhaps under the Security Service, if it had known that Irish terrorism was to be a main national preoccupation for at least the next 30 years. So reorganisation now on these lines for counter-terrorism is not entirely out of the question; indeed it is to be hoped that small centres of expertise on Islamic terrorism have already been created somewhere. But wholesale reorganisation around terrorism seems impractical, for far more reasons that can be adumbrated here. Treverton, though quite radical on intelligence reform, put it neatly before 9/11: ‘the capacities embedded in existing intelligence organizations are both powerful and hard to create, so caution is called for in demolishing them in favor of something new while we are yet so uncertain of the world we will confront’.\textsuperscript{19} The private sector, with different traditions of reorganisation and organisational fluidity, might well reorganise, but can run greater risks of disaster than governments.
Even more hesitation must apply to facilitating the Mark 2 system through reorganising the intelligence community to include more weighty representation for law enforcement. Some of this is already provided, by the FBI’s full membership of the American community and the NCIS’s attendance at the British JIC when necessary. In Britain the various police forces’ Special Branches have also always had feet in the two worlds of intelligence and policing. Giving the many law enforcement organisations a stronger representation in the machinery of the ‘old’ intelligence world would be possible, but quite a change. Despite its involvement in counter-terrorism, law enforcement is still directed principally against crime for financial gain, intrinsically rather different from intelligence’s main targeting on the world of international politics, potential and actual violence and national security as a whole. The objectives and cultures of the two communities are different, and some continued separation is probably sensible, rather than expanding the JIC, for example, into a new mega-community. Possibly a deconstruction of the present intelligence community may eventually be called for, as is perhaps suggested in Robert Steele’s analysis, but it is difficult to see this in the short or medium term.

Counter-terrorism may indeed call for some overlap or revised demarcation between the FBI and CIA, but on the whole the intelligence and law enforcement communities should retain their separate identities. Indeed one effect of 9/11 may be to reverse slightly the trend of recent years towards more coverage by the ‘old’ intelligence communities of their ‘new’ criminal targets. This conservative view applies even more to redrawing institutional boundaries between intelligence and government information-gathering outside law enforcement.

So the IT vision should be applied to broadly the present intelligence structures and not to revamped arrangements. On purely technical grounds this should not pose special problems. The whole concept of an overarching ‘system of systems’ is geared precisely to coping with organisational diversity and the heterogeneous IT that it produces. For such a system an American writer on military command and control distinguishes the different stages of interoperability, integration and interdependence, and argues that these are achievable through a suitable central effort with three characteristics: first, ‘a substantive blueprint for centralised guidance and decentralised execution’, which ‘allows local flexibility to accommodate local needs’; second, dedicated funds to support progress in ‘core activities, such as exercise, experimentation, and interoperability or integration augmentations [to already existing systems]’; and, third, ‘developing trust over time’ by ‘pushing for the common good’ and ‘providing funding for “common good” investments’. Interoperability should be regarded as ‘a process rather than a decision’.
These axioms seem equally applicable to IT for counter-terrorism. They all relate to matters of management, human attitudes and the right kind of central oversight, rather than technological limitations. They accord with the private sector doctrine that IT revolutions promote managerial revolutions, but depend on managerial acts of faith to initiate them properly. IT provides the possibility of new ‘virtual’ communities of analysts, but the opportunities will not be grasped without a commitment to new ways of working. Managers have to ‘think out of the box’ of well-tried preconceptions. So the managerial ‘vision thing’ for the IT vision is a matter of cultural change, putting new wine into the old bottles of a largely unchanged structure. But anyone can talk of cultural change. What does it actually mean for counter-terrorism?

This is where the Mark 1 and Mark 2 solutions diverge. The present writer’s belief is that a campaign for cultural change is possible and desirable within the normal intelligence community; that the Mark 1 system of systems could be pursued with visionary enthusiasm. He is doubtful whether a cultural change of this kind spanning both intelligence and segments of law enforcement and other government data is possible or indeed desirable. Law enforcement intelligence is a developing specialisation, but in democracies it seems undesirable as well as impractical to conflate responsibilities geared to national security too closely with law enforcement’s main task of ‘crime-busting’. Better horizontal flows between the two specialisations are indeed needed for counter-terrorism; the point was made repeatedly in President Bush’s national address in September 2002. But it will need to be pursued on a more pragmatic basis than in the Mark 1 vision. Suggestions in this sense are made later in this essay. Otherwise it now concentrates on the vision for the intelligence community itself.

CULTURAL CHANGE AND THE INTELLIGENCE COMMUNITY

The essentials of intelligence culture need to be maintained: in particular the assumption that intelligence is dedicated to understanding and forecasting objectively, with some freedom from the responsibilities of policy advice, decision-taking and execution. Intelligence has to be close to policy with only a wafer-thin gap from it, but with a gap nevertheless between making key intelligence judgements and deciding what to do about them. This is not peculiar to intelligence, but applies equally to other government information specialisations – the British Office for National Statistics, for example. But it is particularly relevant to counter-terrorism where threat assessment and tactical warning are necessarily close to action, and some distinction between intelligence and action needs to be preserved. I have argued
separately that this characteristic needs propagating as a ‘world standard’ for intelligence everywhere, but that is not the theme here.23

Nevertheless, if intelligence is to realise IT’s potential, data needs to become seen more often as a common asset of ‘virtual communities’, and not a single-agency possession. This is in some ways a frightening vision, violating most of the canons of clear responsibilities, source protection and avoidance of duplication. It would need very careful handling in many ways, including the preservation of professional standards in the citing of evidence; otherwise there could be analytical chaos. Yet it must be recognised that, even with the importance of source protection, intelligence’s traditional distinction between ‘published’ reports and ‘unpublished’ material limits horizontal flows more than is always necessary. Secrecy breeds an unusually intense sense of belonging, but to the agency, not the abstraction of the community. Other agencies may be partners but are sometimes seen also as competitors. Yet serving one’s intelligence collaborators may sometimes be more important nationally than serving one’s non-intelligence customers, and the needs of the two for accessing data may be quite different. The IT vision for counter-terrorism points to a heightened degree of ‘community consciousness’.24

This is not a special problem for intelligence, but applies to all kinds of public service. According to an academic writer on public administration, getting agencies to work together is a matter of behaviour and process, rather than structure. It needs ‘managerial craftsmanship’. Collaboration is not going to happen overnight, but is a long-term process that turns on ‘creating a climate of trust and joint problem solving’. The writer describes this as building up an ‘Interagency Collaborative Capacity’. If true of all government, secrecy and history make the difficulties apply to intelligence in spades.25

In encouraging a greater ‘community’ aspect of intelligence culture something can be learned from the three armed services’ progress over the past 50 years with what the British call ‘jointery’. Military power has been increasingly recognised as a unity, and not as separate categories of land, sea and air operations; recent British defence doctrine for expeditionary warfare is a current example. The military have adapted accordingly. Military specialisations and separateness have not been superseded, but have come to be seen increasingly as parts of some larger whole. Navies, armies and air forces still prize formal responsibilities and command intense single-service loyalties, very similar to those of intelligence agencies; but these have been accommodated in recent years with the development (in the British case) of joint force commanders, a mixed-service helicopter force, RAF aircraft deployed on naval carriers, and the creation of some other fully integrated joint-service organisations, including some in intelligence.
The shift of assumptions has been facilitated by a mixture of doctrine, training linked with appropriate personnel policies and central influence. Community measures to emphasise intelligence’s unity might be considered under these same general headings.

**Doctrine**

Intelligence has little in the way of comprehensive doctrine. The streetwise wisdom of the civilian agencies is rarely formulated in doctrinal terms. Military intelligence has its doctrine, but it is purpose-designed for military settings and training, bringing control to the confusion of battle. In so far as there are received assumptions about intelligence as a whole, they tend to emphasise ‘rational’ frameworks: the military intelligence cycle, the importance of customers’ requirements and priorities; the role of EEIs (essential elements of information); collection plans; ‘intelligence architecture’. Democratic accountability and legislation have also contributed a characteristic emphasis on the roles and propriety of individual agencies. Thus the British Parliament’s Intelligence and Security Committee recently felt it right to publicise its regret that GCHQ accounts are not acceptable to the Comptroller and Auditor General, since audit ‘cannot correlate the physical assets…with the supporting accounting records’. Resource accounting has ‘highlighted the poor asset tracking system’ and ‘forced a culture change’ – not the kind of cultural change advocated here to combat terrorism. Academic writing has contributed substantially to a more subtle understanding of the intelligence community, but has said relatively little about the problems of inter-agency relationships within it.

Professional doctrine cannot be invented overnight. But to reflect the ‘community consciousness’ advocated here two general points might be developed.

The first is that intelligence’s roles of truth-seeking and truth-marketing do not lend themselves entirely to an apparently ‘rational’ and controllable view of its dynamics. All successful knowledge processes seem to thrive on a degree of creative disorderliness and opportunism, sacrificing some order and control for the greater good of creativity and insight. Intelligence is not divisible into neat boxes. Both collection and analysis need initiative, as well as responses to formal requirements. There has to be some kind of order, control and direct responsiveness to customer needs, and developing ‘intelligence architecture’ with these objectives has been a worthy discipline. But perhaps the architecture has to be baroque or rococo, rather than classical. The knack of success is striking the right balance between entrepreneurial local initiative and central control.

The second, related, point is that the accepted typologies of agency specialisations are correct as far as they go, but are simplifications. Some
inter-agency boundaries are rooted in history rather than rational divisions of effort. Where boundaries do follow distinctive differences in skills, the different kinds of covert collection still support each other synergistically more extensively than is often acknowledged; code-breaking for example has been greatly influenced historically by the acquisition of data by Humint and other means, as in the breaking of the German Enigma cipher in World War II. Some kinds of modern technical collection – line-tapping, bugging, outputs from remote sensors, computer hacking, perhaps ‘deep mining’ of the Internet – defy any neat single-agency categorisation, though the US has devised the term Masint (Measurement and Signature Intelligence) to cover some of them. Collection is partly a set of techniques, but is also a capability for opportunistic information-gathering by any means that come to hand, as illustrated in the impressive Cold War history of the CIA’s Directorate of Science and Technology. Similarly, most worthwhile single-agency analysis actually has an all-source purview. Mutual support between its different elements is a key element of intelligence power. Depending on the effectiveness of inter-agency cooperation, this national power is something more (or less) than the sum of its parts.

Human Resources

Organisational culture is influenced in a host of practical ways, and there can be no simple template for promoting community consciousness. But some practical measures could spring from turning accepted assumptions about intelligence organisations on their head. Almost all nations view civilian intelligence employment as a matter of working in one specialist organisation separate from others, with its own distinctive recruitment, training, pay, conditions, career prospects and promotion procedures. The general assumption is that intelligence is a single-trade profession. In the UK the individual organisations have been quite good at training and attachments that expose their professionals to the ‘real world’ outside intelligence, and they have also had some leaders brought in from other parts of government. But historically they have had fewer exchanges within the intelligence community itself; no one except Sir Dick White has ever been head of two British agencies in succession, and as far as can be judged from published CVs no other head of agency has ever worked for any length of time in any of the others. In the US there is more mobility at the top level, but single-agency careers still appear to be the norm below it.

Yet the assumption that a professional life is based on a single agency is not incontestable. In another not totally dissimilar field Britain has a single Government Statistical Service deployed in a variety of government departments. It is not impossible to visualise intelligence similarly as a
single (admittedly larger) National Intelligence Service, divided for convenience into its separate components, each with their individual and distinctive skills and characteristics, but with common conditions, experience and standards where practicable. The military intelligence specialists would necessarily be in a rather different position, but they too could be accommodated in the vision. New ways of developing and utilising a more community-based professionalism might then suggest themselves, for example:

- Provision for ‘equal opportunities’ in pay and prospects between those in small intelligence organisations and those in larger ones. For many years in Britain it was argued that the small Defence Intelligence Staff found it more difficult to recruit and keep people of high talent than the other, larger members of the intelligence community. If analysis now needs more attention than formerly, why not start by offering it parity with the wider intelligence community in pay, prospects and opportunities for inter-agency promotion?

- Mobility of specialist skills between organisations. Linguists are the most obviously redeployable specialists; a system of common recruitment and conditions might facilitate movement to meet changing operational needs. Similarly there may be advantages in making some provision for voluntary switching between specialisations, hypothetically, for example, between Sigint and imagery interpretation.

- Common training at various levels. The different elements of the US community each have their own powerful training organisations, and invite selected members of others to their course; but it is puzzling to the outsider that the US, as the intelligence superpower, does not have a single national intelligence staff college for the whole community. Britain might consider some ad hoc joint service training of this kind; so too could smaller countries. At lower levels, individual British agencies are said to have applied modern management training exercises to produce better internal communication and ‘bonding’; perhaps this training could also be applied on a community basis to produce the same effects on inter-agency relations.

- Planned cross-postings as part of the career development of future senior officers; experience in another intelligence agency would be a desideratum for senior promotions in the parent organisation. This was a recommendation in 1996 of the American Brown-Aspin Commission on Intelligence, but seems to have vanished without trace.
These suggestions apply directly to the intelligence community; the Mark 1 IT vision and not the Mark 2. Yet viewing intelligence professionalism in this more integrated way could have a bearing on the latter. There is no reason why the intelligence specialists in law enforcement should not have some place in a wider intelligence career structure, and some advantage if they were. The professional techniques and standards are virtually identical with some of those in the intelligence community. Horizontal data access between this ‘old’ community and its newer law enforcement counterpart would be encouraged by more staff exchanges and progressions. The writer has argued separately for a wider all-source analyst career in Britain on ‘difficult’ foreign areas, a career which would perhaps include the research and analysis professionals in the Foreign and Commonwealth Office. The inclusion of law enforcement intelligence specialists would add another dimension. To put such bread-and-butter proposals into a wider context: governments’ need to work with intelligence’s techniques and objectivity against difficult targets – whether terrorism, crime or the many others – is increasing. Twenty-first-century governments need to treat intelligence power with increasing seriousness. This means reviewing the ways in which they deal with the profession of those who elect to be part of it.

It may well be argued that informal arrangements already exist for most of the above; that standardisation between agencies is the last thing intelligence needs in an age of devolution in other government services; that the sheer size of intelligence communities precludes this approach in the US and UK (though not in smaller countries, especially where intelligence structures are still evolving); that with modern mobility the idea of careers and career prospects is outmoded – people apply for particular jobs and then move on. All this may be true. Nevertheless, if IT has the technological potential to revolutionise counter-terrorism and intelligence in general, some radical thinking about intelligence’s human dimensions is called for to realise it.

Central Influence

At a technical IT level, introducing the ‘system of systems’ approach considered here needs a central overview with a capacity to develop blueprints, provide funding, and kick-start and oversee the concept generally. At a human level the complementary move towards greater community consciousness requires a similar central influence. Some actual central authority is needed for both, but providing any authority of this kind is a problem for intelligence almost everywhere.

In the US the future of this ‘centre’ still remains largely a matter of guesswork. Thus 9/11 has given an impetus towards central direction; the present DCI appears to exercise considerable personal authority; and
enhanced power for the post figured among the recently stated Presidential objectives. But it is too early to say whether central authority will be permanently strengthened. The new Department of Homeland Security may be improving intelligence’s cooperation with law enforcement, though if changes have been made they have not yet received much publicity. At a technical level within the intelligence community itself its Intelink (its own intranet) may already contain some elements of a ‘system of systems’, and the defence-oriented Joint Worldwide Intelligence System is said to demonstrate a considerable degree of community collaboration. But American intelligence and law enforcement as a whole may just be too large and diverse to preclude any real change in the centre.

In Britain the authority within intelligence has moved in recent years towards the post of Intelligence Coordinator, which has been filled in varied ways and is now combined with that of the JIC Chairman. Worries were expressed some time ago by the Parliamentary Committee about a perceived ‘void in the centre’, though British arrangements there have been so fluid in recent years that judgements should probably be deferred. It is, however, a good sign that the Cabinet Office team tasked with developing community IT has recently been strengthened.

Moreover, 9/11 has recently produced one UK development which may be significant both for intelligence and for much wider areas of counter-terrorism. A new Cabinet Office post has been created at top, Permanent Secretary level with responsibility for intelligence and security matters including defence against terrorism, and the occupant (Sir David Omand) will be able to influence not only IT in the ‘old’ intelligence community but also to encourage bridges between it and law enforcement. He is operating in the wider context of the present British government’s longer-term commitment to ‘joined up government’ – the use of IT to simplify its dealings with citizens by eliminating multiple contacts with different departments – so presumably he will have some influence over inserting counter-terrorism’s requirements into this IT strategy, with suitable safeguards.

Nevertheless the practical difficulties and the problems of reconciling counter-terrorist IT with individual privacy and legal constraints in modern democracies are enormous. Creating a common pool of data on terrorism, with all manner of safeguards, can be pursued in the intelligence community with visionary enthusiasm, and one hopes it will be. By contrast its extension to areas of law enforcement and other government information, though equally relevant, still probably has to be pursued more pragmatically. Outside the intelligence community the vision of the common IT pool is still probably a vision too far.
CONCLUSIONS

Effective counter-terrorist intelligence seems to lend itself particularly to advanced IT. Intelligence is often seen as a matter of human brainpower. But bringing technology properly to bear is now of at least equal importance. Counter-terrorism appears to put a special emphasis on accessing and relating different kinds of data residing in different organisations. Developing IT ‘systems of systems’ to provide interoperability, integration and interdependence between these separate databases may be the key to greater overall effectiveness.

Modern writing on the information revolution suggests that the real problems in exploiting it to the full are managerial and human rather than technical. Managers are urged to ‘think out of the box’ in these matters. In this spirit this essay suggests shifts in the concept of ‘intelligence power’, incorporating:

- Doctrine that emphasises the unity of this power, and lays less emphasis on formal divisions in its processes and the separate disciplines within it.
- Practical personnel policies designed to develop a more holistic view of the intelligence profession and thereby promote the greater ‘community consciousness’ needed to develop community IT to the full.
- The right degree of central influence and leadership backed by an appropriate degree of authority.

This approach is advocated as the managerial/human component of developing an IT ‘system of systems’ for the intelligence community itself. It does not offer a solution to the (greater) problems of providing this community with IT interaction with law enforcement and other government data relevant to counter-terrorism, but its proposals could have some useful spin-off effects in that direction.

NOTES

I am particularly indebted for advice from the late Colonel K.R. Cunningham, US Army War College. I am also grateful for helpful comments from John Morrison and Robert Steele. Responsibility for the views expressed is of course mine.

1. Text of address by Robert David Steele at St Antony’s College, Oxford, 12 June 2002. For his views in detail, see the speaker’s On Intelligence: Spies and Secrecy in an Open World (Oakton, VA: OSS International Press 2001).
3. Ibid. p.98.
10. For a discussion of RMA and references to its literature, see Michael Herman, Intelligence Services in the Information Age: Theory and Practice (London and Portland, OR: Frank Cass 2001) Chap. 3.
11. Part of the vision could also be to link intelligence assessment automatically to menus and options for decision-taking; a counter-terrorist equivalent of the military ‘sensor to shooter’ harnessing of battlespace IT. But this is not pursued here.
14. The present American Defense Secretary is said to have complained recently to the DCI that his briefing on national missile defence had been chaotic since, because of compartmentalisation, no analyst could present the total picture. (I am grateful to Robert Steele for this example.)
15. Herman, Intelligence Services in the Information Age (note 10) Chap. 12.
18. Other current British examples of intelligence and law enforcement connections on terrorism are the National Counter Terrorism and Security Office (NaCTSO) manned jointly by police and Security Service officers, and the Police International Counter Terrorist Unit, also with Security Service representation (Cabinet Office Report, The UK and the Campaign against International Terrorism: Progress Report (Sept. 2002). <http://cabinet.office.gov.uk/reports/terrorism>.
20. Admittedly the discipline of detecting terrorists is not unlike law enforcement’s detection of serial killers; but these are still a small minority of criminals.
23. Herman, Intelligence Services in the Information Age (note 10) Chap. 1.
28. Herman, Intelligence Services in the Information Age (note 10) pp.86–90.
31. For a discussion of the political problems of data security and data privacy in the British objective of ‘joined up government’ on routine matters, see Christine Bellamy, ‘Implementing Information-Age Government: Principles, Progress and Paradox’, Public Policy and Administration 15/1 (Spring 2000).