The National Security Strategy:

Implications for the UK intelligence community

A discussion paper for the ippr Commission on National Security for the 21st Century

by Sir David Omand GCB
Visiting Professor, Department of War Studies, King's College, London

February 2009

Institute for Public Policy Research
Challenging ideas – Changing policy

About ippr

The Institute for Public Policy Research (ippr) is the UK's leading progressive think tank, producing cutting-edge research and innovative policy ideas for a just, democratic and sustainable world. Since 1988, we have been at the forefront of progressive debate and policymaking in the UK. Through our independent research and analysis we define new agendas for change and provide practical solutions to challenges across the full range of public policy issues.

With offices in both London and Newcastle, we ensure our outlook is as broad-based as possible, while our international and migration teams and climate change programme extend our partnerships and influence beyond the UK, giving us a truly world-class reputation for high quality research.

ippr, 30-32 Southampton Street, London WC2E 7RA. Tel: +44 (0)20 7470 6100 E: info@ippr.org
www.ippr.org. Registered Charity No. 800065

ippr Commission on National Security

The ippr Commission on National Security is an all-party Commission preparing an independent national security strategy for the UK. It is co-chaired by Lord Robertson of Port Ellen and Lord Ashdown of Norton-sub-Hamdon. The full Commission membership includes:

- Lord Paddy Ashdown, Co-Chair, former leader of the Liberal Democratic Party and former High Representative for Bosnia.
- Lord George Robertson, Co-Chair, former Secretary of State for Defence and former Secretary General of NATO.
- Dr Ian Kearns, Deputy Chair, Deputy Director, ippr.
- Sir Jeremy Greenstock, Director of the Ditchley Foundation and former British Ambassador to the United Nations.
- Sir David Omand, former security and intelligence coordinator in the Cabinet Office and former Permanent Secretary in the Home Office.
- Lord Charles Guthrie, former Chief of the Defence Staff.
- Lord Martin Rees, President of the Royal Society and Master of Trinity College, Cambridge.
- Sir Chris Fox, former Chief Constable of Northamptonshire and former President of the Association of Chief Police Officers.
- Professor Michael Clarke, Director, Royal United Services Institute, and Professor of Defence Studies at King's College London.
- Professor Tariq Modood, Director of the Leverhulme Programme on Migration and Citizenship, Bristol University.
- Constanze Stelzenmüller, Director of the Berlin office of the German Marshall Fund.
- Professor Jim Norton, former chief executive of the Radio Communications Agency and now at the Institute of Directors.
- Ian Taylor MP, Chair of the Conservative Party Policy Task-force on Science, Technology, Engineering and Mathematics, Conservative MP for Esher and Walton and former minister for Science and Technology at the Department of Trade and Industry.

ippr would like to thank EDS, Raytheon Systems Ltd, De La Rue and Booz Allen Hamilton for their generous support of the Commission's activities. For more information on the work of the Commission please go to **www.ippr.org/security**

The views in this paper are those of the author alone and are being published here in the hope of advancing public debate. They do not represent the views of the Commission panel or the views of any sponsoring organisation.

Introduction

On 19 March 2008, Gordon Brown presented a White Paper to Parliament that served as the first comprehensive attempt to distil a 'National Security Strategy' for the United Kingdom (Brown 2008). The starting point for the strategy is the existence of a fixed and unwavering obligation on the part of government to protect the British people and the British national interest. However, the strategic analysis then goes on to assert that the nature of the threats and the risks the UK faces have changed beyond recognition in recent decades, so confounding all the old assumptions about national defence and international security.

As the strategy makes clear, new threats demand new approaches. A radically updated and much more coordinated response was called for by the Prime Minister and sketched out in the White Paper in relation to both international and domestic defence and security concerns. This policy brief, prepared as a submission to the current ippr Commission on National Security in the 21st Century, seeks to extend that analysis into an examination of the implications of the National Security Strategy for the UK intelligence community.

The paper is organised into three linked sections to try to answer the following questions:

- First, what are the big picture messages from the National Security Strategy that the members of the UK intelligence community might – and should – focus on as most relevant to their work?
- Second, how might the future development of the work of the intelligence community, and the organisation of that community, be influenced not just by those demands but by the challenges of operating in a 21st century environment and with new technologies?
- Finally, how will these developments affect public perceptions and public trust in the work of the intelligence community?

Although the analysis is confined to the British experience, many of the factors identified are likely to be equally relevant to the intelligence communities of the UK's allies and partners.

1. Key messages to be drawn from the National Security Strategy

There has been a wide measure of agreement among commentators that the National Security Strategy has identified the most significant security risks – threats and hazards – that the UK is likely to face in the coming years (see ippr 2008, Kearns and Gude 2008). The threat from international terrorism and from proliferation of the means of causing mass disruption is already present. There is general recognition that major changes will flow from the diffusion of power to the rapidly growing economies of China and India. Likewise, the growth of the influence of non-state actors, be they terrorist or insurgent groups, international criminal gangs, global multinationals or non-governmental organisations, will profoundly influence international affairs. Governments now have to live with the rapid flow of ideas as well as people and capital, and to recognise, for example, that a speech or the publication of a book, film, newspaper, or even a cartoon, can have immediate and violent consequences on the other side of the world. Abroad has come home.

Issues such as global energy and raw material security, as well as access to water and most recently to basic food staples, will become increasingly important, particularly as the stresses likely to be caused by global climate change become more apparent. Some low probability events, particularly were they to involve terrorist use of weapons of mass destruction (WMD), would be so catastrophic as to justify preventative and preparatory steps being taken now. And affecting attitudes to these risks is the growing realisation that as our societies become more sophisticated they become potentially more vulnerable to disruption. These are all now commonplaces of modern thinking about public security and are well registered on the radar screens of the intelligence world. They will form the staple diet for much of the future work of the Joint Intelligence Committee (JIC).[1]

The years ahead will also hold significant opportunities as well as risks, particularly as we benefit from rapid advances in fundamental technologies. There will be unexpected winners and losers from global developments in economic, social and public health fields as well as in the traditional defence and security fields. The overall outlook for national security is therefore hard to forecast, and certainly harder than during the Cold War era of East/West confrontation. This suggests that far greater attention will need to be paid to building up comprehensive horizon scanning and early warning systems.

The UK National Security Strategy does try to identify high-level themes that should help organise thinking about future security needs. Implicit in the strategy are three key concepts, discussed below, that will be particularly relevant to the work of the intelligence community in years to come:

- a redefinition of national security in the direction of embracing the idea of human security
- an endorsement of the adoption of anticipatory policies towards future threats, and
- a recognition of the importance of national resilience, given the inherently greater vulnerabilities to disruption of modern networked and interdependent societies.

A redefinition of national security

Perhaps the most fundamental shift that is to be found in the National Security Strategy is in the definition of national security itself. As the UK White Paper puts it, the state has traditionally been the focus of foreign, defence and security policies while national security has been about the protection of the state and its vital interests from attack by other states. Now, the concept has broadened to cover the responsibility of government to tackle a range of threats to individual citizens, families and businesses. Governments have to manage these risks ‘so that people can go about their daily lives freely and with confidence, in a more secure, stable, just and prosperous world’, to quote the broad security aim of the United Kingdom (Cabinet Office 2008: 5).

One example of this is the priority the strategy gives to supporting communities in resisting violent extremism and terrorist coercion. The objective is to have communities, both at home and in countries of interest abroad, that are strong enough to counter radicalisation and extremism and that are prepared to cooperate with the security authorities to offer information and assistance. Evidently there is the need for the security and intelligence authorities to support such efforts – and as a consequence also to operate in ways that enhance community confidence in the authorities and in the protection they can offer against the extremists.

At times the work may be dangerous, carry significant risks, and overseas it may well involve military force, but it is not conducted in a traditional battle-space. The security and intelligence capability that is needed is what General Rupert Smith has called the ability to ‘operate among the people’, including when operating overseas with peoples of very different outlook, customs, history and culture (Smith 2005: 278). Again, increased demands must be expected on the intelligence community to support the required levels of understanding and to provide specific, accurate and timely targeting information that allows action to be taken within acceptable limits of possible collateral damage (this is discussed in the final section of this paper).

[1] The JIC is part of the Cabinet Office and is responsible for providing Ministers with coordinated interdepartmental intelligence assessments on a range of issues of immediate and long-term importance to national interests, primarily in the fields of security, defence and foreign affairs. The Committee periodically scrutinises the performance of the Agencies in meeting the collection requirements placed upon them.

Another feature of the world described in the National Security Strategy is the blurring of traditional dividing lines: for example between domestic and overseas theatres of operations; and between the worlds of intelligence, security and law enforcement. There are public expectations that government will be able to provide threat warnings and advice on how risks to individuals and businesses can be minimised both at home and when travelling or working overseas. And when things happen to affect the citizen anywhere in the world, such as the tragic terrorist bombing of a tourist bar in Bali, the intelligence agencies should not be surprised when public opinion demands inquiries by oversight committees into their work, into what they knew and what they might have been expected to know that could have allowed the attack to be anticipated. There is an increased challenge here for the intelligence agencies in creating a supportive and informed opinion of their work while safeguarding their sources and methods, without which effectiveness would rapidly diminish.

For those who may be concerned that taking such a human view of national security is broadening the term too much, the application of a principle of subsidiarity may reassure. Authority and information will need to be pushed down to enable local problems to be tackled at a local level, but at the same time national authorities must seize the issues that have international dimensions (and local impacts), such as terrorism, narcotics, illegal immigration and organised crime. The national intelligence authorities will be expected to both ensure that the local enforcement level – including police, border forces and other local authorities – have the necessary information, and to help manage the international dimensions of these domestic threats. These responsibilities are likely to accentuate the shift away from the highly restrictive 'need to know' culture of the traditional intelligence world to what US Director of National Intelligence, Mike McConnell, has called the 'responsibility to provide', a phrase that captures the spirit of the new approach to the provision of intelligence for the purposes of public protection (McConnell 2007).

There considerations will, of course, make it even more important that the UK Agencies continue to develop their networks of contacts with their counterparts around the world, reaching well outside the traditional circle of 'close allies'.

Adopting anticipatory policies

The second 'big idea' driving modern security thinking follows logically from such a train of thought. It is the value of anticipation, in the proper sense of that word. Not just to be able to make predictive judgements about events but to realise what the world would then look like and to identify and implement policies that would reduce the risk to society, both by prevention where that is possible and by preparation where not. Risk is the product of the likelihood of an event, the vulnerability to the impact of the event and the effects of the impact itself should it occur.

Acting in advance to anticipate potential trouble can thus help in three ways. It may be that the intelligence will allow disruption of the threat or at least swing the odds against an attack. It may be possible to act to reduce vulnerability on that threat axis. Then there is the need for rapid situational awareness as an operational threat situation develops, drawing on deep prior understanding of the groups involved, their motivations, aim and techniques. From such assessment should flow operational decisions on alert and warning states, deployments and counter-measures, including science and technology programmes. Finally, there is the value of having longer term analysis of terrorist capabilities and intentions to inform investment in the 'protect' and 'prepare' strands of the Government's counter-terrorism strategy, itself a key component of the National Security Strategy.

Another priority identified in the Strategy (although not described in these terms) in relation to the overseas theatres that are likely to be of enhanced concern in the years to come is a 'responsibility to prevent'. The Strategy calls for the UK to work more closely with its allies and partners to use power and influence responsibly in what has become a highly interdependent world. Picking up on the earlier theme of anticipation, this would include early engagement with nations working to prevent state failure, to inhibit conflict, to help stabilise regions in conflict and to provide conditions where development can progress. There is also increased recognition of the importance of tackling the causes of violent extremism and supporting fragile states in strengthening their governance and promoting economic development. The 'tool-box' therefore needs to contain the full range of instruments ranging from aid and development assistance to military intervention.

As far as the intelligence community is concerned much of this is very familiar, but it must be expected that there will be additional, and demanding, requirements for strategic intelligence appreciation going well beyond the military domain. The intelligence world is still grappling with how best to support civil efforts, including connecting with non-governmental organisations and the private sector security companies working in troubled areas, in terms of their increasing demands for intelligence support as well as their own specialised knowledge and experience that can provide fresh insights.

As already noted, these anticipatory approaches will require the intelligence agencies to engage in more horizon scanning and early warning activity. The National Security Strategy is clear that security is to be considered both in relation to future threats and future hazards (that is, risks arising from natural causes rather than hostile human design). How best to organise horizon scanning in the future is an open question. Would it be better, as some nations are doing, to build upon the established processes of intelligence assessment and warning indicators that have long existed in the defence and security field (for example through the JIC), or to run a parallel civil horizon scanning process linked more closely to the JIC process? There are many subjects where open, or at least, non-secret sources will be sufficient, but there will remain threats for which secret intelligence will be needed and can have unique value. The greatest added value of the secret part of intelligence comes, of course, from the fact that for many of the topics of most pressing interest there are active measures being employed designed to hide or disguise the information being sought. That will particularly be the case where an aggressive opponent is deliberately trying to conceal his intentions.

These features of future national security work will not just generate greater pressure for secret intelligence. Government can also be expected to want the ability to pre-empt threats by authorising covert actions. Such secret agency has in the past ranged from disruption operations against proliferators, terrorists and drug smugglers to back-channel contact and negotiation in circumstances where governments cannot afford to be seen to be directly engaged. These are likely to be even more valuable capabilities in the future world described in the National Security Strategy.

Building national resilience around a risk management approach

The justification for the adoption of an anticipatory approach resides in the nature of the risks to our societies themselves, and flows from a recognition that advanced societies are more vulnerable to disruption as they become more networked and IT-dependent.

Even relatively small-scale attacks can lead to significant cascading failures in interconnected networked systems. In the future such attacks may well be delivered through cyberspace. A requirement set out in the National Security Strategy is therefore to build up national resilience, defined as the ability of society to withstand disruption and to be able to bounce back into shape as quickly as possible. Such considerations emphasise the value of improved strategic foresight and adequate forewarning of strategic developments in the level or type of threat facing our societies, such as anticipating the spread of chemical, biological, radiological or cyber-attack technology. Even when the threat cannot be eliminated, as was the case with the threat of terrorist attacks on UK transport infrastructure, it should be possible with good intelligence assessment to act in advance so that the effects of an attack can be mitigated. The live exercise held on the London Underground, thankfully before the bombing attacks in 2005, illustrates this. Intelligence assessments on such matters – and we are talking here about human judgements with all their potential flaws – could well have major strategic significance for government.

In the United Kingdom, the MI5 Security Service has set up the Centre for the Protection of National Infrastructure (CPNI) to offer advice on physical and personnel security for the operators of the critical national infrastructure (CNI): the essential services such as power, telecommunications and finance without which the economy cannot function, and which are now largely run by the private sector. The CPNI also brings together expertise from within MI5 and the police and from the Government Communications Headquarters (GCHQ) and the UK Signal Intelligence (or Sigint) agency, to advise government and industry on cyber-security and to investigate attacks and intrusions, an important developing role for the intelligence community. Such activities make the workings of the intelligence community much more visible than they ever were during the Cold War to a wider range of stakeholders across government, and in private industry, commerce, local government and emergency services.

In this context the importance of reinforcing the psychological dimension of national resilience needs emphasis, that is, bolstering the fortitude shown by ordinary people working through periods of uncertainty and disruption and keeping normal life going. How the Government uses its intelligence in communicating an accurate, alerting but not alarming assessment of the situation to the public is crucial, and as seen in the run-up to the Iraq war may not be easy to achieve. As noted above, there are public – and quite possibly unrealistic – expectations to be met that government will be able to provide threat warnings and advice on how risks to individuals and businesses can be minimised. The intelligence community will have to take care that government does not oversell the degree of certainty that any intelligence-based warning system can provide. Promoting the idea of risk management was identified earlier as a key aspect of national security strategy, and that applies not least in the intelligence world.

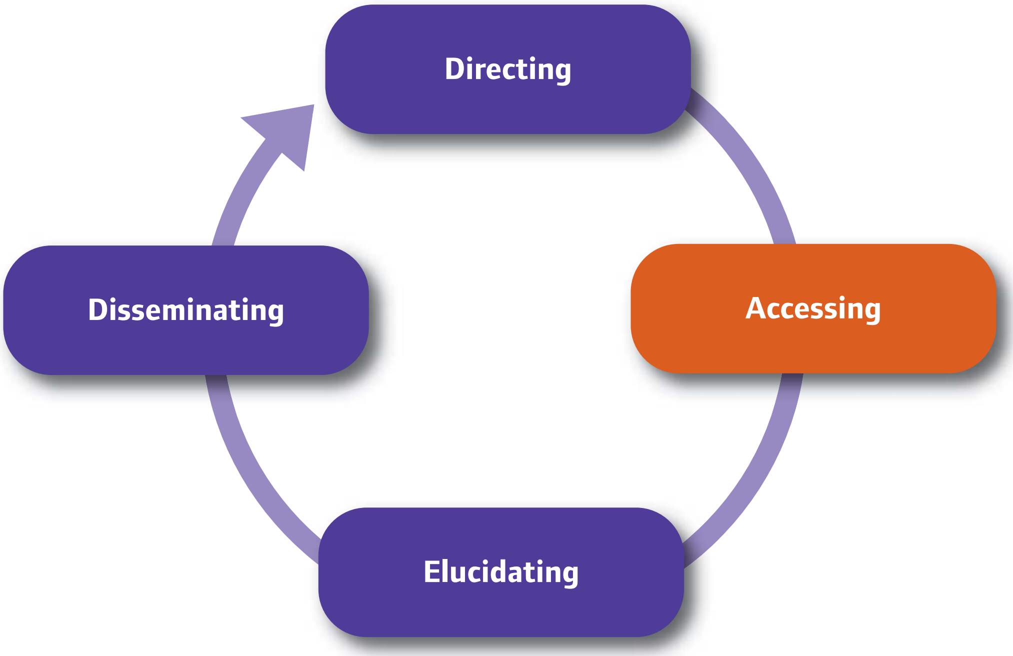
If government follows the logic behind these three ideas – citizen focus, anticipation and resilience – then there will be a number of implications for the way that the intelligence community organises and conducts its work. In addition to the effect of national security policies, the intelligence world is also subject to profound changes in technology (and to the use of technology by its targets). The next section considers these factors together to look afresh at the cycle of intelligence activity as it may develop over the next few years, from setting requirements to delivering product.

2. Rethinking the cycle of intelligence activity

What is meant here by the 'intelligence cycle'? During the Cold War, intelligence activity tended to be discussed in term of a cycle of activities. For example, NATO developed and used a characterisation of the organisation of intelligence activity that started with the setting of requirements for intelligence collection and ended with the dissemination of the finished product to the intelligence staffs of the NATO military commanders. Such a cycle is generally described in terms of *direction* that sets the requirements and priorities for intelligence agencies, who then engage in *collection* of intelligence, the *processing* of that intelligence and subjecting it to *analysis* and bringing different lines of reporting together for *all-source assessment* and finally the *dissemination* of the finished intelligence product. This was an essentially linear process, with user feedback at the end to curl it round into a cycle. Different staffs were engaged at each stage, and in most cases there was a clear separation between single-source raw reporting and all-source assessment, between collectors and analysts, and between analysts and customers for the intelligence.

It is still possible to look on intelligence activity in these terms. But the reality of what staff in the intelligence community do seems to be increasingly different from what the cycle outlined above might suggest. In a post-modern spirit, therefore, rather different terms may be helpful in describing some key components of the cycle so that thinking about the developments to be expected over the next few years is not unconsciously narrowed by the familiarity of the discourse, for example through using words like collection and analysis. Indeed, this paper suggests that the future cycle that will support the National Security Strategy is really best thought of as an interactive network rather than a cycle.

Figure 1: Traditional intelligence cycle



Access

A version of such a modern intelligence cycle is given in Figure 1 above. It is a loop, but for the purposes of discussion, let us break into it at the function labelled *Accessing*. The word 'access' rather than the more traditional 'collection' has been suggested, since it carries the double meaning of 'that which is capable of being reached' and 'that which is approachable in different senses'.

The main point to be stressed here is that the intelligence requirements of those designing and implementing modern national security measures will be based on three types of information: traditional secret sources, open sources, and a third category of personal protected data.

The heart of secret intelligence lies in the recruitment of human sources and the interception (and where necessary decipherment) of communications. In addition to the original human intelligence (Humint) and signal intelligence (Sigint) there is now satellite and photo-reconnaissance (Imint), radar and electronic intelligence (Elint) and measurement and signature intelligence (Masint). These categories provide the basis for recruitment, skill development and organisational structure for national intelligence communities. Nations have differed in whether some or almost all these activities have been under the wing of national defence, diplomatic or interior ministries, but the fundamental organisational structures based on classic types of source remain similar.

However, the volume of information provided by those secret sources is increasingly dwarfed by the availability of open sources of information (Osint). Before the internet age, Osint provided a valuable cross-check and supplement to all-source secret intelligence assessment, for example through monitoring of overseas broadcasts and media. Now, vast quantities of information about target groups and countries, their economies, culture, physical geography and so on are available not just centrally but at any access point to the internet.

Self-regulating internet tools such as Intellipedia (an adaptation of Wikipedia) have found application, at least within the US intelligence community[2]. And intelligence targets also use the internet, as seen by the imaginative use of websites by Takfiri jihadists to promote radicalisation and recruitment,

[2] See http://en.wikipedia.org/wiki/Intellipedia

maintain contact within networks and disseminate information about targets, tactics and weapons. An entirely new branch of intelligence work is therefore having to be created to access, monitor and exploit such material. This information revolution does not supplant the need for more traditional forms of secret intelligence, but it is no longer the poor relation.

To the huge changes happening in the world of Osint must be added the growth of a third category of information from which intelligence for national security may be derived, one that might be labelled 'protected information', or Protint. This is personal information about individual that resides in databases, such as advance passenger information, airline bookings and other travel data, passport and biometric data, immigration, identity and border records, criminal records, and other governmental and private sector data, including financial and telephone and other communications records. Such information may be held in national records, covered by Data Protection legislation, but it might also be held offshore by other nations or by global companies, and may or may not be subject to international agreements. Access to such information, and in some cases the ability to apply data mining and pattern recognition software to databases, might well be the key to effective pre-emption in future terrorist cases.

Such sources have always been accessible to traditional law enforcement seeking evidence against a named suspect already justified by reasonable suspicion of having committed a crime. However, application of modern data mining and processing techniques does involve examination of the innocent as well as the suspect to identify patterns of interest for further investigation. Obtaining international agreement on the sharing of such data will become increasingly important in order to ensure access to these vital sources. Privacy issues also arise over other sources of information on the movements and activities of individuals, revealed by technology such as CCTV or automatic number plate readers, again with future potential for smart recognition software to be applied to mine such data for intelligence and law enforcement purposes.

The realm of intelligence operations is of course a zone to which the ethical rules that we might hope to govern private conduct as individuals in society cannot fully apply. Finding out other people's secrets is going to involve breaking everyday moral rules. So public trust in the essential reasonableness of UK police, security and intelligence agency activity will continue to be essential. A significant challenge supporting the National Security Strategy will be how the intelligence community can access the full range of data relating to individuals, their movements, activities and associations in a timely, accurate, proportionate and legal way, and one acceptable in a democratic and free society, including appropriate oversight and means of independent investigation and redress in cases of alleged abuse of power.

As the author has argued elsewhere, it would not be a complete answer, but it would help if there were greater recognition that members of the intelligence community do, as part of their everyday professional life, follow a set of ethical norms set firmly within the framework of human rights (Omand 2006). Even the United Nations has accepted the value of intelligence in combating terrorism and even a violent business such as war can have its ethical guidelines. Those charged with the oversight of the intelligence community would be well advised to have in mind a set of guidelines such as the following:

1. **There must be sufficient sustainable cause.** Does the scale of potential harm to national interests that is to be prevented justify developing and deploying national intelligence assets with all that that is liable to bring in its train? Passing this test is not just about grasping immediate advantage; it is also about ensuring that the development and deployment of such intelligence capability is likely to further national strategic objectives in the longer term.

2. **There must be integrity of motive.** Are the advantages sought justifiable in terms of the public good, are the motives of all concerned what they appear to be and is there integrity throughout the intelligence process?

3. **The methods to be used must be in proportion to the seriousness of the business in hand,** using only the minimum intrusion necessary into the private affairs of others.

4. **There must be proper authority.** Is there an authorising process at a sufficiently senior level with accountability within a chain of command and appropriate oversight?
5. **There must be a reasonable prospect of success.** Are the risks of unintended consequences, or of political or diplomatic damage if exposed, acceptable; can the golden rule 'do unto others as you would be done by' be applied?
6. **The recourse to the methods of secret intelligence must be a last, not a first, resort** in meeting the need for information. Is there no reasonable alternative way of acquiring the information from less sensitive or open sources?

Such principles should apply to how the three source categories of information input into the intelligence process are accessed. There will inevitably be overlap between the work of those involved in 'access' and the domain of the intelligence analyst, who will often be best placed to steer the access in near-real time. It is therefore probable that a new function of access or mission management will be developed: one that can access, manipulate and collate the required sets of information using the most effective set of sources. The ability to conduct intelligence work in a hostile environment (the Cold War paradigm), behind enemy lines as it were, will remain an important part of the total picture. But much of the information needed, for example, to track terrorist groups, including their financing, resides in open sources, on the internet and in databases within our own societies, where the barriers to entry for the intelligence authorities are of a very different kind and call for access expertise of a different order. To these access challenges must be added the difficulties of keeping up with new communications technology.[3]

Nor is the world of human intelligence immune from the pressures of new national security threats. A significant challenge for humint agencies, as discussed by ex-Chief of MI6 Sir Richard Dearlove, is the process of adjusting operations from the recruitment of a small number of very long-term 'deep penetration' agents to the many short-term, often casual, sources of the international counter-terrorist paradigm (Dearlove and Quiggin 2006). The humint world also has to deal increasingly with the ethical issues surrounding their activity against non-state targets such as those that arise from running participating agents inside violent terrorist and narcotics gangs.

The National Security Strategy argues that traditional dividing lines are blurring: for example between domestic and overseas theatres of operations; and between the worlds of intelligence and law enforcement. Access to intelligence for the purposes of counter-terrorism illustrates the interconnections between domestic and overseas theatres.

The sought-for intelligence to help pre-empt terrorist networks will come from two directions: modern, professional intelligence using all the human and technical tradecraft of which the agencies are capable; and information volunteered from within local communities in rejection of the extremists and their ideology.

One obvious need in support of the strategy is to create the ability to work intelligence targets across the divide between national and overseas theatres. Terrorist cases that arise domestically are likely to have links to extremist circles overseas, and such links will have to be pursued overseas. Likewise, intelligence operations overseas may directly illuminate emerging domestic threats. Joint operational pursuit of cases will become more common, and the same pressures will be felt by the UK's intelligence allies and partners.

As already noted, modern intelligence access will often involve intrusive methods of surveillance and investigation, accepting that in some respects this may have to be at the expense of some aspects of privacy rights. This is a hard choice, and goes against current calls to curb the so-called surveillance society, but following the logic that flows from the National Security Strategy, it is greatly preferable

[3] These include voice over the internet protocols (VOIP), packet switched networks, and the general volume of modern communications, together with the ubiquity of commercially available hard encryption.

to tinkering with the rule of law, or derogating from fundamental human rights. Being able to demonstrate proper legal authorisation and appropriate oversight of the use of such intrusive intelligence activity may become a major future issue for the intelligence community, if the public at large is to be convinced of the desirability of such intelligence capability.

Encouraging the provision of information to the authorities will involve maintaining community confidence in the actions of the state, including in the protection provided by the framework of human rights and the quality of justice. Good pre-emptive intelligence reassures the community by removing the extremists and by disrupting potential attacks without having to fall back on blunt discriminatory measures that alienate moderate support within the community, and on which effective policing and counter-terrorism depends. Means as well as ends will be held to matter here.

Elucidation

Next we turn to the analytic processes that are central to the derivation of meaning from this mass of secret, open and protected information. In Figure 1 this part of the cycle is labelled *elucidation* since that word helpfully carries the meaning of throwing light upon and explaining that which is in shadow.

We have to recognise that modern national security strategies place two types of demand on the intelligence community to elucidate a complex world. These represent forces pulling the analytic community in two different directions, with the recent emphasis on using intelligence for the purpose of immediate action (for counter-terrorism, counter-proliferation, narcotics interdiction and so on) pulling one way, and the need to provide strategic awareness of longer term developments of wider security interest pulling the other. However, in both cases the task is to generate and test hypotheses in order to provide the best explanation possible consistent with the observed facts and the deepest possible understanding of the individuals, groups and regions concerned, their people, language, customs and mores.

The first shift in emphasis is to intelligence for what has been described as 'action-on'. This is intelligence that is sufficiently accurate, precise and timely to allow someone to use it for the purposes of public protection, or in pursuit of a tactical military objective. That shift has profound implications for the extent to which the intelligence community must work as a community and the stronger relationships with law enforcement and homeland security policymakers that are required, along with the wider relationships with overseas services. It has implications for a change in relations with the media, for the role of oversight and for the degree of public confidence in the ethics of the intelligence community.

As already noted, much of this work will rest on open sources of information. Often the assessments concern mysteries relating to how situations may develop rather than the secrets of what already exists – the plans, orders of battle and equipment tables of the classic assessment function (which are still needed, of course, since inter-state conflict has not disappeared with the end of the Cold War). The demands on the analyst community of such work are very considerable, not least because the local players themselves may not fully understand the dynamics of the situation. It will not just be a question of what analysts 'know' but what they 'understand'. More attention will be needed in future on training analysts to think and to be conscious of the methodologies they are using, and their pitfalls. And a larger proportion of the budget will have to be spent on the activities that allow meaning to be derived from accessed intelligence as against the mechanisms of access themselves.

The UK already has a well understood mechanism for strategic intelligence assessment in the JIC. The key characteristic of the JIC is that its judgements are arrived at in discussion between the intelligence professionals and their senior policy customers from the Cabinet Office, Foreign and Commonwealth Office, Ministry of Defence, Home Office, HM Treasury, Department of Business, Enterprise and Regulatory Reform and elsewhere. All have to dip their hands in the blood of the collective judgements, however unwelcome they may be. This aspect is, as far as is known, unique around the world. The task of the professionals is to keep judgements anchored to what the intelligence actually reveals (or does not reveal) and keep in check any predisposition of policymakers to exaggerate the situation. The policymakers in turn must ensure that the judgements actually try to address the issues that need answering rather than just those on which their intelligence sources are richest, and help the professionals couch any warnings justified by the intelligence, without their seeming to attack the policy itself and thus risk compromising the neutrality of the JIC.

The processes supporting the JIC and the range, type and form of reporting issues have evolved over the years and will need to evolve further in the course of applying lessons from past experience, not least over Iraqi WMD assessments. As observed earlier, it does already have a formal responsibility for early warning, and could thus provide at least the basis of a wider horizon-scanning effort in support of the National Security Strategy if the Government so chose.

Debate will no doubt continue about the added value to Ministers outside a time of crisis of the short JIC strategic assessments with their consensus key judgements (as revealed, for example, in the Butler Report; see Butler *et al* 2004). In comparison, the US system provides much more detailed National Intelligence Estimates, including more detail and sometimes presenting alternative views where these are held by some but not all members of the US intelligence community. The JIC output may have to become a more mixed one to respond to the different demands. However, there is one clear advantage that the UK system has: it forces senior, and very busy, officials to work actively together in the JIC on key judgements for an afternoon every week of the year, which has generated a political-military community that is uniquely well informed about each other and that has high levels of mutual understanding and trust. That is one reason why the UK has been able to work across boundaries on counter-terrorism in ways that other nations with their more compartmented traditions have not yet achieved.

At the operational level the UK now has the Joint Terrorism Analysis Centre (JTAC). This operates on a joint multi-agency basis, and its assessments are issued on its own authority, under the supervision of the Director General of the Security Service. JTAC is a relative newcomer in comparison with the JIC, and fills a gap that was opening up at the operational level for detailed and timely counter-terrorism (CT) assessment. Other subjects, such as counter-proliferation, would benefit from a similar approach, but the small size of the UK's analytic community on such topics may make that impracticable. To overcome this difficulty, areas of secure cyberspace where work in progress can be posted for peer discussion by a chosen group of analysts are needed, and other ways of forming virtual analytical centres using advanced secure technology will have to be developed. All this calls for the sort of changes that Tom Fingar, Chairman of the US National Intelligence Council, has recently described under the rubric of analytic transformation (see Fingar 2008).

International intelligence cooperation on counter-terrorism has developed considerably since the attacks of 11 September 2001. Sharing assessments and warning and alerting information is likely to increase in importance in years to come. In considering the implications of this, for example in terms of cooperation at a European level, it may be helpful to think of the intelligence community serving three levels of government: these are the classic distinctions between working at the strategic level, at the operational level and at the tactical level, with the distinguishing feature between the levels being the time horizon of the customers receiving the intelligence:

- The National Security Strategy calls for strengthening of UN, NATO and EU capabilities and decision-making. At the strategic level, this will require nations to share assessments to guide policymaking, for example on future protective or border security measures, on collective measures on criminal justice informing judgements over trade-offs between civil liberties and security, or on trade-offs between data protection and privacy and the effectiveness of intelligence-gathering. National security issues will need to be backed by policies at a European level, and these are only likely to follow if there is shared appreciation of the potential risks that are to be managed. For instance, the UK has been active already in building up the EU Joint Situation Centre so that nations can share their strategic assessments to inform debate in the Council of Ministers and thus help a consensus to emerge at the European level. The pressure will grow for more intelligence-based assessments to be shared in this way.

- At the operational level, an international demand is likely to remain for sharing of timely all-source analysis to support operational decision-making (in the way that JTAC does). It is encouraging that a number of countries are creating their own inter-agency mechanisms for operational threat assessment, even though the exact geometry will vary from country to country. What matters is that mechanisms develop over the next few years that will help nations to act consistently when faced with the same threat, an example being the nature of warnings to travellers in countries affected by terrorism or natural disaster.
- At the tactical level, individual lines of intelligence are generally going raw to other intelligence specialists, to defence staffs or to policy customers who are themselves expert and able to interpret the material. Such information-sharing with allies and partners to support counter-terrorist operations overseas is endorsed by the National Security Strategy. But sensitive tactical details of current operations on the ground are only going to be exchanged internationally between the services concerned where there exists prior trust that operations – sources and methods – are not going to be compromised by precipitate unilateral action, or unwise media briefing. It takes time, and shared experiences, to build up such trust. The UK is fortunate in that its own agencies share relationships of trust with many sister agencies on a global basis. These relationships are developing and deepening and that trend will need to be encouraged, particularly at a European level. The UK is also likely to face continued initiatives from some of its partners for intelligence and security institution-building at a European level. At the same time, the importance of maintaining close relations between traditionally close allies will not diminish, and may increase under the pressure of national security challenges. Therefore the wiser course for the UK is likely to be to make progress on all three fronts set out above in ways that recognise the nature of the subject matter, and accommodating different national constitutional and historical experiences, but without creating new freestanding institutions.

What will not change in coming years are the many ways in which elucidation can fail to illuminate. The risks of such errors today may be thought to be higher than during the Cold War simply because there is more human judgement to be applied in modern circumstances, and the assessments must inevitably cover more of the nature of mysteries than secrets, to use Professor R V Jones's useful distinction (Jones 1989). Analysts have to be trained to become aware of these pitfalls, and encouraged to think consciously about the methodologies they are following. At each level, getting inside the minds of the adversary is essential, as is understanding the influence of language, culture and geography. A consequence of the nature of intelligence work as it is described here is that there will be relatively less inductive reasoning, and rather more hypothesis formulation and testing, for example in relation to the possible intentions of groups that may not yet themselves know their potential capabilities.

Dissemination

Dissemination describes the policies and processes necessary to get the intelligence into the hands of those who will use it, and sometimes to those who have no idea that they need to know or indeed might prefer not to know the assessments being reached by the intelligence community. The word conveys a helpful sense of sowing seeds for later germination.

There are three points in particular that should be made about the future development of this part of the intelligence cycle. First, as already noted, the shift away from the highly restrictive 'need to know' culture must continue. Today dissemination must be both outwards, including to partners and allies

[4] The various sources of error, including mirror-imaging, transferred judgement and perseveration have been widely studied in the historical literature and in reports such as that of the Butler Inquiry. A summary of the Nicholl Report into lessons from past JIC assessment failures of was released under the Freedom of Information Act by the UK Cabinet Office in October 2007.

overseas, and downwards, where the issues around classification, tear-line reporting and fusion centres[5] are now well discussed in the literature (see for example Sullivan and Wirtz 2008).

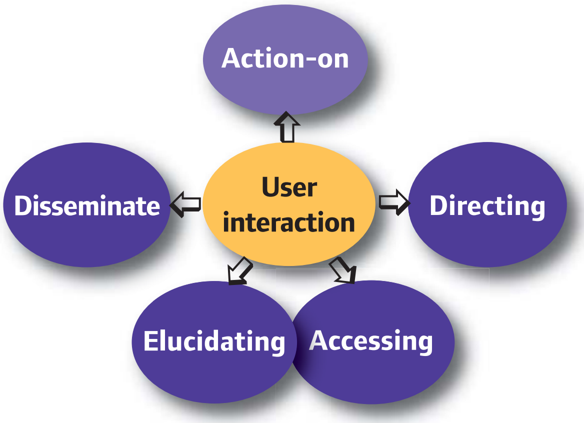
Secondly, although the traditional written intelligence report will remain the staple, the requirement now is also for maps, pictures, biometrics, video and data of all kinds. A supporting infrastructure of secure broadband communications stretching out into the customers' space becomes essential.

Finally, the customer community, especially in the military commands, will have to be increasingly able to rapidly pull the intelligence material needed to generate situational awareness and enjoy the 'Amazon.com' ability to find past products and perhaps be told, as you are when you search for a book on Amazon, which other products previous users of that item also found useful.

Action-on

At this point a new feature is added in to the cycle (shown in Figure 2 below), drawing on the earlier discussion of action-on intelligence.

Figure 2: Intelligence cycle in the 21st century security environment



An increasing effort has had to be put into dealing with 'action this day' intelligence (particularly in the areas of proliferation, terrorism, narcotics and serious crime), as opposed to intelligence to inform policymaking. Armed police storm a house in the suburbs, armoured vehicles appear at the airport, passengers are told they cannot take liquids in hand-luggage, bollards appear in front of public buildings, an air-to-surface missile from a drone precisely targets a vehicle on the other side of the world. These are all visible signs of intelligence being acted on.

During the Cold War such use was normally covert, away from public gaze. Now it could not be more visible. The pressure on the intelligence community to allow its product to be used, including in court, can only increase. The pressure to allow pre-emptive action within the ()geo-location of suspects (as described in Coram 2002). The requirement to be able to integrate multiple sources of intelligence in real time to support operations, whether at home or far off theatres, will increase. The risk management judgements between longer-term exploitation and short term public protection will become harder, as will the trade-offs between security for the source and action-on. There are considerable implications for the intelligence community, and its overseers, in such developments and so action-on issues therefore deserve their own place in the intelligence cycle.

[5] An intelligence fusion centre is a collaborative effort of two or more agencies that provide resources, expertise, and/or information to the centre with the goal of maximising the ability to detect, prevent, apprehend, and respond to criminal and terrorist activity.

Direction

Looking back to Figure 1, the cycle returns round to *direction*, the capacity needed to manage the cycle, including evaluation of intelligence priorities based on a review of the changing security environment. It is not hard to see what should be key priorities from the point of view of the traditional political and military customers. But the broader definition of security we have moved towards means that there will be more customers, covering a wider range of governmental activity, that may benefit from intelligence support. The future threats identified in general terms in the National Security Strategy will have to be turned into specific statements of intelligence priority as part of the normal intelligence requirements process, and regularly reviewed and updated as part of the cycle of intelligence activity.

The directing function is also needed to ensure that the policies being followed by the components of the intelligence community, and the balance of investment between their capabilities, fit the overall likely needs of the National Security Strategy and of external pressures ranging from technological advances to public opinion. In the UK (although not yet in all partner countries) the last few years have seen the development of at least the beginnings of the necessary directing function for the whole national intelligence community.

What will be the resulting shape of the future intelligence community, responding to all the pressures that have been identified in this paper? Will there be pressure to merge the domestic Security Service and the Secret Intelligence Service? Will there be pressure to place all the supporting technology and data management in a single technical agency? Will the UK analytical community be brought closer together? Most commentators, including those within the community, would recognise that what the UK now has is a fortunate result of long experience plus quite a number of accidents of history. However, it is not what would be designed *ab initio* to meet the needs of national strategy in the 21st century. No doubt in the years to come such questions will continue to be posed, driven largely by considerations of economy as well as effectiveness.

The advantage of organising the community around the existing agencies could be seen as comparable to the value from having retained the three fighting services in terms of recruitment, basic training and ethos. That consideration in turn raises the prospect of the development of an increasing capacity to plan and generate force and capability packages on a joint basis, as the UK defence establishment does. An additional consideration, which may assume greater importance in the future, is the widening of the concept of the community for the purposes of planning of communications, security and technological applications for the three secret agencies, and wider engagement with the defence intelligence staff, the Cabinet Office Assessments Staff supporting the JIC, JTAC, analysts in customer departments and in the Serious Organised Crime Agency, the Metropolitan Police and other police services.

User interaction

In Figure 2 the intelligence cycle is represented with a further box highlighted as a connection between the elements of the cycle, representing *user interaction*. Unlike the classic description of the cycle, it is therefore no longer a loop but an interactive network.

The point here is to try to capture the thought that what will increasingly need to be created are virtual communities of users, analysts and mission managers with a variety of access possibilities. There will need to be greater inter-visibility of the work of each of these groups, without compromising analytic independence. The need to respond to the terrorist threat has already driven such changes in relation to that subject, but this process should develop more widely across the national security agenda. To take one national security priority, that of domestic resilience, there will need to be overlapping circles of information reaching all the way out from the secret agencies to the commercial operators of the critical national infrastructure.

3. The implications of more visible use of secret intelligence for public security

The National Security Strategy explicitly states that it is 'clearly grounded in a set of core values' including 'human rights, the rule of law, legitimate and accountable government, justice, freedom, tolerance and opportunity for all' (Cabinet Office 2008: 6). At the same time, the strategy draws attention to the way that the current jihadist terrorist threat has grown, and to the steps taken to generate actionable intelligence, to invest in electronic borders, identity cards and counter-terrorist legislation and to encourage the development of liaisons with a wide range of countries (some at least that have very different security and intelligence traditions from those of the UK).

Looking ahead, it is likely that there will continue to be a vigorous debate over whether the measures being taken, and the activities of not just the UK intelligence community but also its allies and liaison partners, are consistent with those core values (see Oborne 2006 and Mueller 2006 for a comparison of UK and US debates on these issues). The intelligence community will continue to have to grapple with issues of proportionality and necessity over its methods, and over the use made of its intelligence. As already noted, the advanced technology now available to the intelligence community is particularly valuable in providing early clues to the existence of covert networks, but the very effectiveness of these techniques is already rubbing up against feelings of invasion of individual privacy, and worries over the wider uses to which such information might be put.

The present British policy is to accept information from any source that bears on our major interests, at the same time as taking all reasonable steps to promote UK views over acceptable interrogation methods overseas. But will it continue to be sustainable in terms of Parliamentary acceptability that in return British intelligence information should be passed to other countries if that information might lead to action by others that would not be considered acceptable by the UK? As observed earlier, means matter here as well as ends.

4. Conclusion

The first UK National Security Strategy places significant demands on the British intelligence community that will require further developments within that community and in its relationships with its customers. Future challenges for the intelligence analyst will be twofold and will pull in opposing directions: on the one hand, applying the latest electronic technology to work ever closer with the user to generate actionable pre-emptive operational and tactical intelligence; on the other, standing back from the policy hurly-burly to provide deeply knowledgeable and grounded strategic assessments from an independent position of professional detachment.

However, the ultimate object of intelligence will remain to enable action to be optimised by reducing ignorance; and of secret intelligence to achieve this object in respect of information that others wish to remain hidden. The primary purpose of intelligence will therefore continue to be to generate organised information that can be put to use to acquire relative advantage. The future military commander will need more precise intelligence to enable his network-centric systems to function, while the security service, police and border service officer will need more pre-emptive intelligence to protect the citizenry from international terrorism and serious and organised crime, including via counter-proliferation, and to frustrate the ability of terrorist groups, and some states, to acquire means of mass destruction. And the policymakers still need to have professional support to collect and organise information relevant to the decisions and actions that they want to take, and crucially, to some that they may not yet know they need to take. Thus it seems clear that government in the future world sketched out in the National Security Strategy, with the threats and risks it identifies, will have every bit as much need of secret intelligence as in the last half-century.

References

Brown G (2008) 'National Security Strategy statement', March 19, available at: www.number-10.gov.uk/output/Page15102.asp

Butler R, Chilcot J, Inge P, Mates M and Taylor A (2004) *Review of Intelligence on Weapons of Mass Destruction, Report of a Committee of Privy Counsellors,* July 14, London: The Stationery Office

Cabinet Office (2008) *The National Security Strategy of the United Kingdom* London: Cabinet Office

Coram R (2002) *Boyd: The Fighter Pilot Who Changed the Art of War* New York: Little and Brown

Dearlove R and Quiggin T (2006) *Contemporary Terrorism and Intelligence, IDSS Commentaries,* August 7, available at: www.rsis.edu.sg/publications/Perspective/IDSS0782006.pdf

Fingar T (2008) *Speech to the Council on Foreign Relations,* Washington, DC, March 18, available at: www.dni.gov/speeches/20080318_speech.pdf

Institute for Public Policy Research (ippr) (2008) *Shared Destinies: Security in a globalised world, The interim report of the ippr Commission on National Security in the 21st Century*, London: ippr, available at www.ippr.org/publicationsandreports/publication.asp?id=636

Jones RV (1989) *Reflections on Intelligence* London: Heinemann

Kearns I and Gude K (2008) *The New Front Line: Security in a Changing World* London: ippr, available at www.ippr.org/publicationsandreports/publication.asp?id=588

McConnell M (2007) 'Overhauling Intelligence' *Foreign Affairs,* July/August

Mueller J (2006) *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats and Why We Believe Them* New York: Free Press

Oborne P (2006) *The Use and Abuse of Terror: The Construction of a False Narrative on the Domestic Terror Trail* London: Centre for Policy Studies

Omand D (2006) 'Ethical Guidelines in Using Secret Intelligence for Public Security', *Cambridge Review of International Affairs*, 19/ 4 (December), pp. 613-28

Smith R (2005) *The Utility of Force* London: Allen Lane

Sullivan J P and Wirtz J (2008) 'Terrorism Early Warning and Counterterrorism Intelligence', *International Journal of Intelligence and Counter Intelligence,* Vol.21, No.1, Spring