It may be helpful to summarize here the main conclusions about the institutions, activity and output of the government intelligence model examined here: the UK-US (and Commonwealth) community, which also illuminates many features of Western intelligence and some aspects of modern intelligence power everywhere.

The system

Intelligence developed slowly as a permanent institution from the mid-nineteenth century to the beginning of the First World War, with more rapid growth thereafter, culminating in the satellite surveillance and increased power of electronic collection in the last quarter-century. This development has been matched by the growth of other organized government knowledge, such as government statistics and law enforcement intelligence. Like these other institutions, the government intelligence discussed here is a system of organized information-gathering, analysis and forecasting; like them, it serves government's executive functions but with an all-important institutional separation from policy-making and decision-taking. Thus peacetime intelligence is separate from diplomacy; similarly wartime intelligence is organizationally distinct from Electronic Warfare and other 'combat information' collected and used as integral parts of military operations.

Intelligence's broad subjects are foreign targets of all kinds and internal security threats (including terrorism), with much overlap between the two. In resource terms 'foreign intelligence' on the first group of targets is considerably larger than 'security intelligence' on the second. Within intelligence as a whole there are two other, separable components. The first is information collection, operating without its targets' cooperation or knowledge, usually by special means designed to penetrate secrecy. It is expert on particular techniques. By contrast the second, 'all-source' component is expert on particular subjects, to which the collection effort contributes.
Summary

Most intelligence resources are invested in collection, particularly in the modern Sigint agencies and (in those countries with intelligence satellites or access to their results) in those developed for imagery collection and interpretation. These technical agencies combine collection with processing, and disseminate some important single-source intelligence direct to users. This single-source service applies particularly to direct support of diplomatic negotiations, irrespective of subject.

Collection as a whole has two broad categories of output: 'observational' intelligence on 'things'; and 'message-like' intelligence derived from access to human communication of some kind, typically through securing documents, eavesdropping on conversations or deciphering communications. Most collection, especially the message-like material, is vulnerable to countermeasures. The consequent need for special secrecy pervades the whole intelligence process.

Predominant as collection is, definitive intelligence inputs to users are from the second (much smaller) stage of all-source analysis and assessment. Modern collection agencies are skilled in interpreting their own material, but the all-source stage has to weigh and finally assess multiple intelligence sources, along with material of non-intelligence origin such as diplomatic reporting, the media and contact with the enemy in war. Exploiting the many kinds of ‘open’ data bases now becoming available on a commercial basis adds to this importance of the all-source stage. One of the strengths of the UK-US-Commonwealth system is that the specialist collectors of secret intelligence do not normally have final responsibility for assessing the significance of their own material. The all-source melding of all available evidence provides a much broader concept of intelligence than the Soviet idea that it was essentially the product of secret collection. All-source intelligence assessment can cover a wide variety of overseas subjects, and is not just dealing in others’ secrets. But its authority with governments is greatest where there is some connection with national security, and a need to cope with organized foreign concealment or deception.

Purposes

Intelligence targets range widely, but a feature of the overall effort is the considerable investment devoted to defence intelligence on foreign armed forces and armaments in their widest aspects, including the international arms trade and foreign insurrection and civil war. One of

1 Soviet battlefield intelligence (razvedka) was of course based on normal military all-source principles
intelligence’s largest if normally unspectacular commitments is meeting the peacetime needs of its own state’s armed forces and being able to support them in war.

On these and other subjects intelligence’s main purpose is to assist its users’ actions, but how this happens is almost infinitely variable. Some intelligence is used immediately, while more of it has cumulative effects, or educational or psychological values which influence action indirectly. Some warning coverage is a precaution against threats which never materialize. Much output of all kinds has no discernible use at all. Intelligence shares with all other information these characteristics of apparent waste, unpredictable value and serendipity.

Nevertheless the general effect is to optimize national strength and international influence in peacetime and promote the effective use of force in war and other conflict. It is part of the state’s defences against internal threats. In both war and peace the main impact is cumulative and undramatic; though intelligence can sometimes determine the way in which wartime campaigns are fought, and can be a major factor in counter-terrorism.

There are also secondary effects. National intelligence is used for international security as well as narrowly national purposes. It also supports national information security, through counterespionage, counterintelligence and defensive advice and standards-setting; the standard required by national governments for their defensive information protection is a factor to be considered in determining how much to spend on sophisticated offensive collection. In the Cold War the fact of espionage and other intrusive collection reinforced East–West threat perceptions. In war intelligence also operates as a threat, inhibiting targets’ freedom of action and the efficiency of their command, control and communications systems.

Furthermore there is a long-running technical contest between offensive intelligence and the security defences of its targets. A small breach in the defences can lead to the ‘expanding torrent’ of offensive intelligence success, which in turn has effects of strengthening its own side’s defensive security. Between long-standing antagonists this intelligence–security contest is supported by an even more specialized counterintelligence campaign in which intelligence seeks to disable or capture its professional opponents. Intelligence has to fight some protracted contests of these kinds at its own technical, professional level, and part of its peacetime resources are employed in this way in maintaining ‘technical continuity’ on its targets and a counterintelligence capability.

Along with these adversarial effects and contests, intelligence also has
its networks of international cooperation. National investments buy more than purely national outputs. The forms of cooperation are influenced by states’ overarching political relationships, but also have some influence on them. Intelligence cooperation tends to be based on professional considerations, particularly the assessment of partners’ information security standards; but it can also be provided or withheld as a means of diplomatic leverage. In close relationships intelligence communities believe they are influencing each other’s national views; the general effect is perhaps to strengthen common perceptions.

Quality

These varied national and international effects are still subsidiary to intelligence’s main purpose: to make its own government’s action better than it would be without it. Its primary concern is therefore with its accuracy, combined with its credibility with its users and relevance to them; it has to be close to them without sacrificing objectivity.

Three sets of conclusions can be suggested to these ends. First, ‘warning failure’ against surprise attack tends to reflect basic misperceptions about targets, as well as failures in the operation of the community machinery. Warning should not be separated from long-term assessment; the numbers engaged in both should be kept small. A nucleus of experienced professional assessors is needed. Some supervision of the interdepartmental machinery is needed to spot weaknesses before they are found out by intelligence failure. These conclusions over ‘warning’ have implications for assessment as a whole.

Second, the problem of users’ preconceptions has particular salience for defence intelligence, whose organizations are large and influential parts of the intelligence community. They have never been regarded as one of its strong points. In the Cold War a lack of independence and professional quality made them unduly influenced by armed forces’ and defence industries’ vested interests in the Soviet threat. The antidote is more corporate identity and professionalism, and greater national esteem. At least in Britain, this means recognizing that all-source analysts warrant the same pay and promotion prospects as the professional collectors.

Third, there is great value in the UK–US–Commonwealth device of interdepartmental national assessment which tests departmental assumptions and provides policy-makers with agreed intelligence inputs. The machinery for it depends on a delicate balance between collegial participation by the intelligence community and leadership from a central assessment group. The composition of the central group needs
a balance between professional assessors and those with wider experience. There is also the question whether the interdepartmental assessment ‘college’ should include representatives of policy-making departments (as in the influence of the Foreign and Commonwealth Office within the British system), or be limited to genuine intelligence organizations: whether national assessment is a process of ‘intelligence assessment’, or of ‘government assessment’ which engages all government knowledge and opinion. A final question is how the detailed all-source analysis needed to underpin national assessment should be organized. Arguably the US structure, in which CIA’s Directorate of Intelligence can study foreign targets as single entities, has advantages over the British arrangements which divide them organizationally into separate political, military and economic segments.

Management

The intelligence community has moved in the direction of sizeable, high-technology production plants. Its management needs to evaluate effectiveness and efficiency, as well as quality of output. One conclusion for management is that the ‘intelligence cycle’ is a useful cybernetic metaphor, provided that emphasis is placed on intelligence’s initiative; the driving force is intelligence’s search for users’ reactions to the service provided to them, rather than reacting only to users’ ‘requirements’. Intelligence has entrepreneurial instincts for maximizing user satisfaction, and these need to be given scope.

Another conclusion is that, although intelligence processes can be costed in some detail, the ‘internal’ information content of output cannot be quantified in any consistently helpful way. The same applies to the use made of it. Yet many ‘externals’ of intelligence production and supporting activities can be counted and costed, and they provide additional, useful management information.

Finally, an intelligence ‘market’ between producers and users would not be an effective way for deciding intelligence investments and resource allocation. The complexity of the community and the short-termism likely in a market combine to make it seem both impracticable and undesirable. Yet users must be encouraged to think more seriously about the costs of what they are asking for and receiving.

These assumptions suggest that intelligence can usefully absorb some of the cost-conscious, results-oriented culture being encouraged throughout the modern public service, but without devising any special management ‘system’ to embody it. At the community-wide level the main management problems are indeed of a different kind. Intelligence
communities are diffuse, and some issues are too big to be resolved merely through single-agency bids or inter-agency consensus. Both the British and the US communities need stronger strategy and planning to enable intelligence to be handled as a national resource. Modest measures towards a more effective community in this respect would be some strengthening of central staffs, and the creation of greater ‘community consciousness’ through planned inter-agency exchanges for career development. Though excessive centralization must be avoided, both nations may also have to face up to vesting effective managerial responsibility for the community in one place.

Within agencies the normal principles of good management apply. Intelligence employs ordinary people, in large numbers and with wide varieties of skills and expectations. There is still a high proportion of lifetime careers in single organizations. The most distinctive feature of the organizational culture is intelligence’s secrecy and the sense of difference and mystique it produces. Secrecy combines with long-term employment to produce high but slightly brittle morale.

The insulation caused by secrecy makes it important for intelligence to seek ideas from ‘outside’ and to draw on modern management practices of ‘informal’ organization, though there are valid reasons for preserving some aspects of tight control and formal delineation of responsibility. The main bearing of secrecy is however on the application to intelligence of the modern public service-wide style of results-oriented management, in which institutions have been enjoined by government to emphasize contracts, targets and monetary incentives rather than commitment. As long as espionage (or whistle-blowing) is a genuine threat to intelligence sources, management has to take a special interest in its staff, and exercise an unusual degree of surveillance of their official and private lives. Intelligence is particularly vulnerable to discontented employees, and the necessary surveillance of its staff is tolerable only if combined with fairness and humanity. More than most organizations, intelligence has to be a genuinely caring employer.

1990s and beyond

Chapters 19 and 20 suggested national and international needs and a strategy to meet them. Intelligence has to be judged increasingly by its peacetime usefulness; though it is also a necessary support for armed forces, a precautionary warning system, and a national capability that can be expanded in these and other unforeseeable directions. The search for measures of cost-effectiveness and cost-benefit fits the increased test of peacetime usefulness, even though the search will never be completely
successful. Reductions in expenditure should be arranged so that, apart from any cuts in security intelligence, the impact falls on collection and not all-source analysis. Analysis needs more attention than it has had. The priority is the relatively inexpensive one of improving its quality, and equipping it to keep pace with the ‘open source’ opportunities now open to it.

Nevertheless collection will continue to be the main intelligence investment. Even with a reduced workforce, major capital investments will continue to be needed to keep pace with targets and grasp opportunities – particularly those open to satellite collection. Apart from meeting narrowly national needs, collection now has the additional role of providing intelligence for the support of UN operations and other aspects of international security. There is a growing onus upon the United States and other effective intelligence powers to develop this international role.

The general effect of intelligence knowledge is also to incline national governments to behave better, in international security terms, than they would without it. Most of the intelligence collection that contributes to this knowledge operates over long distances and is unspecific in its targets. Intelligence as a whole tends to improve international society and does not introduce new tensions within it; it is an unprovocative form of national power.

But part of its collection – admittedly a small part – is more intrusive on its target states, and is liable to contribute thereby to the spectrum of inter-state threats. Extensive Humint attacks on foreign states (not on terrorist or similar organizations) can be perceived as threats of this kind; so too can extensive close-access technical operations, and operations under diplomatic cover or attacking diplomatic premises. Threat perceptions are related mainly to the intensity of these intrusions. States could usefully work towards an international climate that moderates collection of these kinds, restricting it to reasonable limits and genuine needs.