SECURITY SERVICES IN AN OPEN SOCIETY

by

David Charters

> "I've got a story to tell you.
> It's all about spies. And if
> it's true, which I think it is,
> you boys are going to need a
> whole new organization."

Thus spake Ricki Tarr, erstwhile agent of the "Circus", a moribund British secret service. His chilling words sent veteran superspy George Smiley in search of a "mole", a Soviet double agent who had burrowed deep into the heart of British intelligence.[1] Fiction, of course, penned less than a decade after the author, John Le Carré, had written the introduction to a non-fiction account of a real mole: Kim Philby.[2] Coincidence? Hardly, although the secret world is fraught with coincidence, irony and the extraordinary blending of fact and fiction.

The irony is all the greater in this case, for while Canadians watched the serialized novel on television this past spring, a real life drama was being played out in the Canadian courts. Leslie James Bennett, former chief of counter-intelligence in the RCMP Security Service, is suing for libel Ian Adams, author of *S: Portrait of a Spy. RCMP Intelligence - the Inside Story*.[3] The suit alleges that Adams has implied in his "novel" that Bennett was a Soviet agent. Bennett was discharged from the Security Service in 1972 after a four-day interrogation raised doubts about his loyalty, but he was never officially or publically charged with being a spy or a traitor.[4] The libel case has yet to be resolved and it would be inappropriate for this author to venture an opinion on it. But the Bennett case and its supposed fictional counterpart, like the Philby case and the Le Carré novel before them, highlight important issues in the current debate about the role of security services in open societies. This article will attempt to demystify that role and to identify and explain some of the issues and problems confronting both the intelligence community and those who "watch the watchers."

The Intelligence Task

Intelligence is more than just information. It is "the product resulting from the collection, evaluation, analysis, integration and interpretation of all available information which concerns one or more aspects of foreign nations or of areas of operation and which is immediately or potentially significant to military planning and operations."[5] Although this definition emphasizes the military dimension, intelligence takes other forms — political, economic, technological. The principal function of intelligence is offensively to achieve and defensively to avert surprise. It is intended to reduce the margin of ignorance among national security policy makers and in that context it is, as Klaus Knorr observes, the continuation of politics by other means.[6] Surprise can take many

forms, although it is generally the military form which comes first to mind. History is replete with examples of surprise attack, whose consequences need no further elaboration. Today the superpowers rely increasingly on technological means, such as spy satellites, to minimize the possibility of surprise attack at the strategic level and to ensure, by assessing visible military capabilities, that each is abiding by arms control agreements. In this sense, intelligence-gathering plays a major role in preserving world peace. But in the field of intentions, of determining what one's opponent thinks and plans, the satellite is of little use and it is here that there remains a role for the traditional spy.

It should be emphasized that not all intelligence-gathering is, or need be, secret: much of what governments need to know about each other, at least in so far as "open" societies are concerned, may be derived from public sources. An effective intelligence organization will devote the largest proportion of its resources to analysis of material from open sources, thereby defining more clearly the limited areas where clandestine collection may be required. To do otherwise would leave the intelligence service grasping at straws in the dark, with no overtly verified information against which to judge material collected by covert means.[7] Many countries, however, are "closed" and even liberal democracies have secrets. Truth lies protected behind layers of deliberate security. Nowhere is the fog of war more opaque. Consequently, as Hugh Trevor Roper has observed, "So long as governments conceal a part of their activities, other governments, if they wish to base their policy on full and correct information, must seek to penetrate the veil."[8] The United States and Soviet Union commit formidable resources to winkling out one another's secrets, for in the war called peace "the peace is only nominal. War is war, whether declared or not . . . menace can arrive as swiftly as the proverbial bolt from the blue; secret services need constantly to watch for it."[9] Intelligence, then, has an important defensive role, and small as well as major powers are potential targets. Hence, the need for security in otherwise open societies.

Role of Security Services

The principal task of a security service is counter-espionage: to identify and place under surveillance the intelligence agents of hostile powers — many of whom operate "legally" under diplomatic cover — and, if necessary, to frustrate their activities. In the major capitals of the world it is a formidable task, but even in the relative tranquility of Ottawa the RCMP Security Service devotes considerable resources to surveillance of the Soviet KGB and its allied agencies, notably the Cuban DGI and Czechoslovak STB.[10] As Michael Foot observes, however, outside of a tyranny manpower requirements preclude wholesale surveillance of all potential foreign agents.[11] In any case, however troublesome, these agents are probably the easiest to deal with, simply by virtue of the fact that they are foreign and bear some official accreditation by which they become known. A far greater problem is the "illegal", a foreign agent living under assumed identity in the target nation. He or she may have entered the country some time in the past and be working in a trusted position in government or in some other profession which permits access to sensitive information. If undetected at the point of entry, the illegals may work unmolested by the security service. Their only weakness is that sooner or later they may have to com-

municate whatever information they collect to a "legal" or visible foreign agent. Provided the latter are under surveillance, the contact point or means of communication may become known and the illegal identified, neutralized (arrested or deported), or even "turned" to work for the security service.[12]

By far the most serious espionage threat, that suggested in the introduction to this article, is the mole or double agent, the trusted native son working both for his own intelligence or security service and that of a hostile power. Philby is, of course, the classic case, though he is by no means the only one. The mole poses three distinct threats to the host service. First, by passing information to the source of his true loyalty he can disrupt the activities of his assumed employers — their sources are betrayed, their agents captured or killed, their plans leaked and frustrated. It is dangerous work for a double agent since, like the illegal, he or she must maintain some kind of link with or conduit to the rival agency. Security service surveillance or information planted deliberately to identify the source of the leaks may lead to exposure. These risks highlight the importance of the second task — as "agent of influence". Le Carré notes that by designating its intelligence targets, a secret service "declares its own ignorance and thereby points to the areas in which it is most easily deceived."[13] In this case the mole can inflict infinite harm with minimal risk to himself, since contact with the "enemy" agency is not essential. According to Edward Epstein, deception or "disinformation" — the product of a mole's activities — may manifest itself in two forms: first, by hiding, camouflaging or fabricating recognizable items of intelligence, a disinformation plan may induce the target agency to miscount observable data; secondly, where data cannot be concealed, the double agent may mislead or confuse the target service, causing it to misinterpret the intentions of the hostile power. Since matters of motive and strategy are essentially intangibles dealing in shadings of meaning, the disinformation content is not immediately verifiable. The basic requirement for success is a "hinge of reality" — the material and the channels through which it comes must be credible.[14] Here the mole is at a tremendous advantage, for who will know better than he what his government wants to hear and is willing to believe? Moreover, the very nature of his intelligence responsibilities places at his disposal the technical means for creating disinformation and may even permit him to establish contact with "the hostiles" for the alleged purpose of cultivating a high grade source. The deception plan may extend to providing a wall of innocence around the mole while ensnaring an unsuspecting colleague in the web of intrigue. But even if it does not, or if the cover plan fails, all is not lost for even in exposure a mole may play a third, usually unintended, but equally valuable role. As Le Carré explains, "A penetrated secret service is not just a bad one; it is an appalling liability. In place of an all-seeing eye, it becomes a credulous ear and a misleading voice, innocently deceiving its own customers in every sphere of the national security."[15] Penetration on the scale of Kim Philby, once exposed, completely discredits the hapless service in the eyes of its sources (those still alive), its customers and its allies, none of whom will be ready to trust and do business with the service again until a record of reliability has been re-established — a process which might take years. Ironically, then, a mole may do his greatest damage by being exposed or by "surfacing" voluntarily — preferably, for his sake, after escape to the country he served covertly. In the scandalous after-

math, it remains only for indignant politicians and an inquisitive news media to finish the destruction he initiated.

Obviously, security services take precautions to prevent foreign espionage in whatever form it may manifest itself. Preventive security involves essentially three tasks: first, physical security — the protection of government buildings and installations and the classified materials they contain. Positive vetting (or security clearance) of persons with access to classified material is the second task. This is intended to eliminate spies and double agents and to ensure that normally reliable people cannot be compromised and blackmailed into working for hostile intelligence services. The third task is communications security — to prevent deliberate or unintended leaks of sensitive information. This includes ensuring the use of proper voice procedures, codes, cyphers and scramblers; checking that codes and cyphers are changed frequently and have not been broken; "sweeping" buildings for wiretaps and "bugs"; ensuring that "loose talk" is minimized and that classified waste is destroyed. No system is foolproof, of course, and the security service must respond if it suspects that a government department or agency has been penetrated. Where the target is the intelligence community itself, the methods of uncovering a mole are essentially two: first, an internal inquiry, a time-consuming process which could involve retracing the course of all "blown" operations, debriefing exposed agents and informers, searching for disinformation clues and the re-vetting of all personnel — including interrogation of likely suspects. But, as the hunter and the hunted may be one and the same, there is no guarantee of success. The mole, of all possible suspects, will have an airtight alibi. The second method is to penetrate the hostile service, using the information gathered there to identify and eliminate the double agent in one's own. Quite apart from the length of time such penetration takes, perhaps years, it is by far the more dangerous operation: the enemy will be expecting it, watching for it, especially if they have an agent in place to warn them in advance. Once the mole is uncovered, some "cleaning of the Augean Stables" will be required. The kind of wholesale reorganization suggested by Ricki Tarr probably would be unnecessarily extreme. But even a limited internal purge of key personnel would disrupt normal operations for a considerable period.

Were counter-espionage the only task of a security service, its job would be difficult enough. But in the 1960's and '70's security services in western countries were drawn increasingly into the "gray areas" of counter-subversion and anti-terrorist operations. Here they confronted a major dilemma. The societies they are sworn to protect are open, with relative ease of access to information and especially to people. The organizations which threaten them are closed, compartmentalized, often armed and dangerous. They are generally skilled in penetration and in cloaking their intentions and activities in familiar innocent forms.

Terrorism is a case in point. Surprise is crucial to successful terrorist operations, since by secretly choosing the time, place and manner of attack the terrorist hopes to neutralize the potentially greater strength of the security forces which will respond to his action.[16] Furthermore, surprise is central to the psychological impact of terrorism, frequently the principal objective of terrorist operations.[17] Obviously, the most desirable, rational response is to

apprehend the terrorist prior to attack, but as Major-General Frank Kitson has observed, "the problem of defeating the enemy consists very largely of finding him."[18] An efficient, effective terrorist organization will protect itself from such inquiry in two ways: first, by adopting a secure cellular structure which, by reducing internal personal connections, can minimize the hazards posed by the capture of any one member. For years this organizational form protected the Red Brigades from penetration by the Italian security services and in the latter half of the 1970's the Provisional IRA adopted a similar structural pattern.[19] The second way in which a terrorist organization may seek to protect itself is by penetrating the police intelligence and security services. By placing its own members or sympathisers within the anti-terrorist organization, the terrorists can be forewarned of impending security operations — and thereby frustrate or misdirect them — and can identify and eliminate key members of the security forces. Britain's "small wars of decolonization" provide many examples of such penetration and their disastrous consequences, and the accurate targeting of senior security personnel suggests that the Red Brigades have experienced some degree of success in penetrating their opponents.[20] On the need for timely, accurate intelligence in order to pre-empt terrorist activities, and for an efficient security service to prevent penetration, nothing more need be said.

In an open society, however, it may not be possible or even desirable to apply the same techniques to the rooting out of terrorism and subversion as are employed in counter-espionage, because the target of investigation is so different. In the case of the mole, security operations may be confined to the *suspect service or department or directed only against the service of a hostile* power. But in the case of subversion, and counter-terrorism, investigation is directed against part of the nation — the people the security service is supposed to protect.

The definition of subversion is central to the problem. It is possible to provide a clinical, technical description of the process — action taken to acquire "disguised but effective control over a population or group which is supposed to be under the control of some constituted authority."[21] The subversives may use a combination of legal and clandestine illegal techniques to infiltrate and take control of institutions and organizations within society, with the aim of creating a "rival state" which can eventually challenge the power of the incumbent government. The security forces are probably the most important targets of subversion since, without them, a government is powerless to defend itself. It *will not even know it is threatened until it is too late. But the identification of* people and organizations engaged in subversion tends to be subjective. The process is open to abuse since the government or the security service may classify as subversive anyone they do not like. That leaves the way open for harassment of innocent people and legitimate groups, violations of privacy and the host of legal and moral questions that flow therefrom. Furthermore, once exposed, such abuses discredit the security service, with much the same consequences as the exposure of a mole. A discredited service cannot protect a society or itself and leaves both open to exploitation by hostile agents or genuine subversives.

Issues Demanding Answers

The problems discussed above raise one basic question: can an open society defend itself against espionage, terrorism and subversion and still remain open? The author believes that an effective security service need not pose a threat to democracy. But if the freedoms we enjoy are to be preserved, governments might well address themselves to the following issues:

1. How much secrecy is necessary? All governments tend to "overclassify" the paper they produce. A more selective approach to classification might have several beneficial effects. First, less classified material in circulation would mean fewer genuine and embarrassing leaks. Secondly, it would reduce the number of people, especially civil servants, who would have to be security cleared. That, in turn, would mean fewer background investigations, invasions of privacy and files on private citizens. Finally, it is easier to protect a smaller amount of classified material. This approach, combined with a greater effort to explain to the public the need for a degree of secrecy — in short, explaining the threat — and the role of the security service, might produce security, administrative and civil liberties benefits.

2. Who is responsible? A security or intelligence service which is out of control is a menace to the society it is intended to protect. There must be a clearly defined chain of command and responsibility to senior officers of the service and to their political masters, who should be held accountable to the elected body in which they represent the public. If some degree of supervision is deemed necessary, to prevent and to examine abuses, then the composition of any commission should be a matter for careful consideration. A panel of politicians may not be the best safeguard either of civil liberties or of internal security.

3. Overt versus Covert Operations — The nature of espionage, subversion and terrorism demand some covert counter-measures. But, as stated earlier, an efficient service will devote the largest proportion of its efforts to overt operations and should not have to cast its net too wide in the covert sector. Where undercover operations are deemed essential, however, security services require clear directives as to what is and what is not legally permissible. Furthermore, they should not be required to break the law in order to enforce it since, quite apart from the legal and moral questions, violent, subversive, conspiratorial activity is incompatible with the methodical task of collecting and processing information which lies at the heart of security intelligence work.[22]

4. Separation of Powers — Policy-makers might consider whether the same organization should be responsible for collecting and analysing security intelligence and for exploiting it. Clearly, such an arrangement presents a potential danger of a service making work for itself. Law enforcement is a police responsibility which should not be shared with a security service, whose task is essentially investigative.

A liberal democracy will never be completely secure from the threats of espionage, terrorism and subversion. That is the price it pays for remaining an open society. But attention to and, if necessary, positive action on the issues outlined above should go some way to striking a balance between personal liberties and national security.

Footnotes

1. John Le Carré, *Tinker, Tailor, Soldier, Spy* (London, 1974), serialized for television by the BBC (1979) and broadcast by the CBC (May-June 1980).
2. Bruce Page, David Leitch, Phillip Knightley, *The Philby Conspiracy* (London, 1968).
3. Gage Publishing, Toronto, 1977. The book sold some 15,000 copies, but was taken out of circulation when Bennett brought his libel suit against Adams and Gage.
4. *Globe and Mail*, 11 Dec. 1979; *Observer*, 10 Feb. 1980.
5. NATO definition, from P.H.C. Hayward, ed., *Jane's Dictionary of Military Terms* (London, 1975), p. 88.
6. Ray Godson, ed., *Intelligence Requirements for the 1980's: Analysis and Estimates* (New York, 1980), p. 1 and comment by Klaus Knorr, p. 117; Donald McLachlan, "Intelligence: The Common Denominator", in Michael Elliott-Bateman, ed., *The Fourth Dimension of Warfare, Volume I: Intelligence, Subversion, Resistance* (Manchester, 1970), p. 54.
7. Hugh Trevor-Roper, *The Philby Affair: Espionage, Treason, and Secret Services* (London, 1968), pp. 66-67; John Bruce Lockhart, "The Relationship Between Secret Services and Government in a Modern State", *Royal United Services Institute Journal for Defence Studies*, vol. 119, no. 2 (1974), p. 5.
8. Trevor-Roper, p. 66.
9. M.R.D. Foot, "Britain-Intelligence Services", *Economist*, 15 March 1980, p. 52.
10. John Sawatsky, *Men in the Shadows: The RCMP Security Service* (Toronto, 1980), pp. 153-90.
11. Foot, p. 53.
12. Sawatsky, pp. 12-13; John Barron, *KGB: The Secret Work of Soviet Secret Agents* (New York, 1974), pp. 106-7.
13. In Page, Leitch, Knightley, p. 14.
14. In Godson, pp. 123-34. The importance of "disinformation" is discussed in "Spiking the Media", in this issue.
15. In Page, Leitch, Knightley, p. 14.
16. Wayne A. Kerstetter, "Terrorism and Intelligence", *Terrorism: An International Journal*, vol. 3 (1979), p. 109.
17. Paul Wilkinson, *Terrorism and the Liberal State* (London, 1977), pp. 81-82, 110-12.
18. Frank Kitson, *Low Intensity Operations: Subversion, Insurgency, Peacekeeping* (London, 1971), p. 95.
19. Vittorfranco S. Pisano, "The Red Brigades: A Challenge to Italian Democracy", *Conflict Studies*, no. 120 (1980), p. 10; Peter Janke, "Ulster: A Decade of Violence", *Conflict Studies*, No. 108 (1979), p. 17; *Toronto Star*, 29 Aug. 1979.
20. Pisano, pp. 8, 10.
21. Edward Luttwak, *A Dictionary of Modern War* (London, 1971), p. 194.
22. H.H.A. Cooper, "Terrorism and the Intelligence Function", *Chitty's Law Journal*, vol. 24, no. 3 (1976), p. 73; McLachlan, p. 53.