GENEVA CENTRE FOR THE DEMOCRATIC CONTROL OF ARMED FORCES (DCAF)

WORKING PAPER NO. 103

DEMOCRATIC AND PARLIAMENTARY ACCOUNTABILITY OF INTELLIGENCE SERVICES AFTER SEPTEMBER 11TH

Peter Gill

Reader in Politics and Security, School of Social Science
Liverpool John Moores University, United Kingdom

p.gill@livjm.ac.uk

Geneva, January 2003

GENEVA CENTRE FOR THE DEMOCRATIC CONTROL OF ARMED FORCES (DCAF)

WORKING PAPER NO. 103

DEMOCRATIC AND PARLIAMENTARY ACCOUNTABILITY OF INTELLIGENCE SERVICES AFTER SEPTEMBER 11TH

Peter Gill

Reader in Politics and Security, School of Social Science
Liverpool John Moores University, United Kingdom

p.gill@livjm.ac.uk

Geneva, January 2003

DEMOCRATIC AND PARLIAMENTARY ACCOUNTABILITY OF INTELLIGENCE SERVICES AFTER SEPTEMBER 11TH[1]

Peter Gill

Introduction: the need for democratic accountability

In the past thirty years throughout Europe, the Americas and more sporadically elsewhere the issue of how to institute some democratic control over security intelligence agencies has steadily permeated the political agenda. There have been two main reasons for this change. In what might be described as the 'old' democracies (North America, Western Europe, Australia and New Zealand) the main impetus for change was scandal involving abuses of power and rights by the agencies. Typically, these gave rise to legislative or judicial enquiries that resulted in new legal and oversight structures for the agencies, some of these achieved by statutes, others by executive orders. The best known examples of these are the U.S. congressional enquiries during 1975-76 (chaired by Senator Church and Representative Pike), Justice McDonald's enquiry into the RCMP Security Service in Canada (1977-81) and Justice Hope's into the Australian Security Intelligence Organisation (1976-77, 1984-85).

Elsewhere, this shift has been a central, and sometimes painful, aspect of the democratisation of formerly authoritarian regimes, both civilian and military. For example, the death of Franco in 1976 precipitated democratisation in Spain that included the de-militarisation of intelligence (Giménez-Salinas, 2002). Military rule ended in Brazil in 1985 though the military dominated National Intelligence Service (SNI) was not replaced until 1990 as part of a continuing process of de-militarisation (Cepik & Antunes, 2001). During 1993-94 a more rapid transformation of formerly repressive security agencies was attempted in South Africa (Joffe, 1999). The other major examples of this transition since 1989 are the countries of the former Soviet bloc where no agency has been immune from the changes although the amount of real as opposed to nominal reform varies widely (for example, Rzeplinski, 2002; Szikinger, 2002).

---

[1]Paper prepared for the Workshop on Democratic and Parliamentary Oversight of Intelligence Services, Geneva, October 3-5 2002. The Workshop was organized by the Geneva Centre for Democratic Control of Armed Forces (DCAF).

Whether scandal or the democratisation of former authoritarian regimes (and sometimes both together) have been the main impetus for change, the main emphasis of reforms has been on increasing the legality and propriety of security intelligence operations. Although in some cases attention was paid also to the issue of obtaining effective security intelligence (e.g. McDonald, 1981), the overall direction of change was to the better control and accountability of agencies whose past activities had been dominated by the surveillance of political opponents rather than genuine security threats.

But since the September 11 2001 attacks in New York and Washington DC, the debates around security intelligence have shifted to the contemplation of 'intelligence failure' and how future threats can be averted. This is most obviously the case in the US itself but the impact of the global 'war on terror' has been much more general. This repeats the historical pattern in which concern regarding *propriety* has increased following scandals while intelligence 'failures' such as 911 give rise to increased concern with *efficacy*. In this atmosphere it is easy to see how the democratic gains of the last thirty years might be swept away in the naïve belief that agencies 'unhampered' by oversight requirements might somehow be more efficient and effective.

It is a mistake to view efficacy and propriety as being in a zero (constant) sum relationship such that gains in one are outweighed by losses in the other. Rather, they should be viewed as being in a non-zero (variable) sum relationship such that both can be improved. This is not to say that there is no tension between the two: it is quite easy to see how, in the short run, the ability to conduct surveillance of an individual or group may be reduced by the requirement to follow procedures that seek to protect privacy but, in the longer term, such procedures are required if a state is to be entitled to call itself democratic. Such procedures should be designed in order that, even in the short term, the invasion of privacy is proportionate to the alleged threat but also to prevent it being directed at the wrong person or conducted in such a way as to amount to intimidation. Thus legal rules themselves may contribute to efficacy as much as to propriety.

But in the search for better public control of intelligence, improved legal rules alone will be insufficient. The task of democratisation and search for efficacy/propriety includes shifting both the *legal* contexts for intelligence work and the *culture* of the agencies. Although the process of achieving legislative change can itself be difficult

and require considerable political will, there is a danger that, once it is achieved, it will be *assumed* that real change in the agencies and their behaviour will result. This is a dangerous assumption: new laws themselves may only achieve *symbolic* change (Edelman, 1964) so that people can be reassured that problems have been dealt with. If they are not matched by even greater effort in implementing those laws then little that is real may change. Beneath the surface of new laws, what the agencies actually do and how they do it might remain essentially unchanged. Achieving cultural change in agencies that may have long histories of complete autonomy from outside control or influence is a long term project that may require even greater political will than achieving initial legal reform.

It is important to define some key terms (cf. Caparini, 2002). 'Control' is relatively straightforward: it refers to the *management and direction* of an organisation and can be exercised at various levels, for example, if a Parliament passes a law relating to the mandate and operations of an agency then we can justifiably talk of 'statutory control'. Closer to the agency, we might talk of 'executive' or 'political' control where a member of a government (such as an Interior minister or Attorney General) may issue directions to an agency. Then, within the agency itself we might talk of administrative control by a Director including the promulgation of internal regulations and guidelines.

'Oversight' is often used interchangeably with 'review'. This may be because in some languages the terms are interchangeable, for example, in the French version of the Canadian Security Intelligence Services Act 1984 the term *surveiller* is used to describe what is described in the English version as 'review'. In early days of the Act there was some controversy surrounding the role of the Security Intelligence Review Committee (SIRC – see further below). Critics of its activism argued that 'review' was a *post hoc* activity whereas those advocating a more extensive role including, if appropriate, ongoing operations preferred to rely on *surveiller*. Thus the interchangeability of the terms can disguise what is actually an important distinction, as we shall see in the discussion below. For the purposes of this discussion it is useful to adopt Caparini's usage: to use review to describe an ex post facto process and oversight to describe a process of supervision that might include ongoing activities (2002, 5)

Some principles of control and oversight

Even a cursory examination of developments in different countries during recent decades indicates that there is no single 'rulebook' for the design of architectures of democratic control and oversight or review. Clearly, the sets of legal and institutional relationships that emerge in any specific country will be the product of the unique culture, history and politics of those places. Thus, any comparative enterprise such as that providing the inspiration for this DCAF project must start with respect for these varying traditions. However, there is no point in a comparative analysis if the *only* objective is to provide an exhaustive *description* of the variety of practices. If academic social science is to contribute anything to a debate that concerns immediately both intelligence and political professionals then it must be to clarify and explore more general issues pertaining to the governance of intelligence so that they can inform the specifics of debates anywhere.

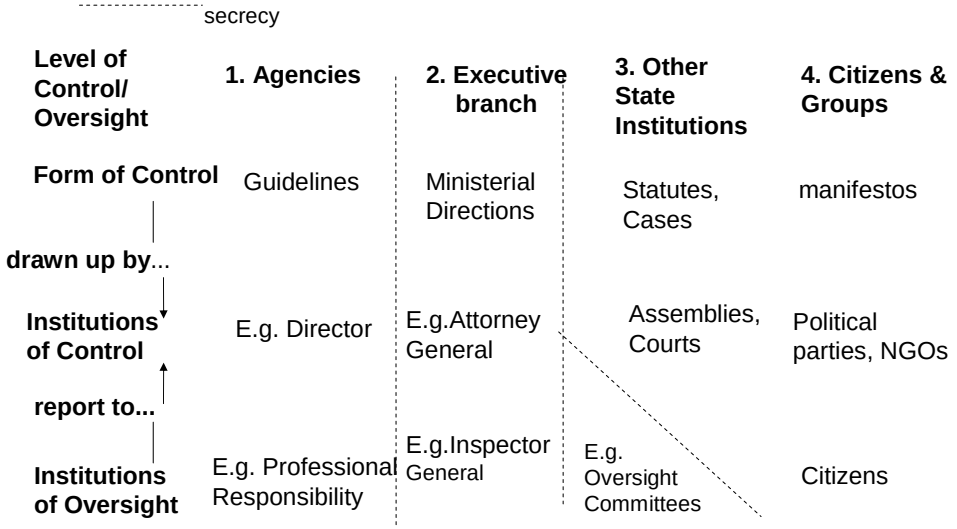
Much can be gained from the comparative study of security intelligence (Hastedt, 1991). The use of security intelligence by states displays certain common features regardless of their precise form, for example, secrecy, a tendency to confuse 'security threats' with 'political opposition' and the use of 'extra-legal' methods to obtain information and disrupt opponents. Also, it is possible to see the development of cross-national intelligence 'communities' so that the differences between national agencies may be less than might be assumed. To be sure, this tendency is clearest within coalitions of nations, for example, the UKUSA pact of anglo-saxon countries, especially their SIGINT agencies or the Warsaw Pact between what were 'counterintelligence states' in Eastern Europe. Elsewhere, and sometimes even within coalitions, there are fierce 'intelligence wars' between agencies but there are clear signs now of convergence between agencies in the context of the globalised 'war on terror' led by a hegemonic United States.

Still, the actual structuring of any particular state's security intelligence agencies and the appropriate forms of control, oversight or review will be determined finally by the particular political culture and traditions of that state. Therefore, it is idle to suggest that states might simply pick and choose from institutions operating elsewhere; political institutions cannot simply be transplanted from one political system to another. But studying institutions elsewhere may well help to prevent a state 'reinventing the wheel': states can learn from each other. So, in this paper, the object is not to lay down some set of hard and fast rules for effective public control; rather, it

is to suggest that there are certain fundamental questions that have to be answered and certain basic principles that can be enumerated based on the study of intelligence reform in several countries.

Figure1: Control and Oversight of Security Intelligence Agencies

Control and Oversight of Security Intelligence Agencies
(Adapted from Gill, 1994)



The Figure 'Control and Oversight of Security Intelligence Agencies' summarises key relationships. The horizontal axis is based on the proposition that 'states' are not single entities: they operate at three main levels, the demarcation between them often indicated by secrecy barriers. First, there is the most secret level occupied by security and military intelligence agencies; second, the executive branch (or government) and, third, the broader array of state institutions including elected assemblies, judiciaries and bureaucracies. Since we are concerned with the issue of public control, we must also include a fourth – non-state – level in our analysis, representing citizens, groups and social movements.

The vertical axis seeks to summarise, first, the different institutions and forms of control that need to exist at each level and, second, the complementary institutions of oversight or review. Forms of control become more specific the closer the level is to the agencies. The manifestos generated by political parties or social movements are

not strictly-speaking a form of ‘control’ because they may have no impact on agencies but they will provide a general set of demands that might at some point inform more specific statutes or court actions. Some Parliaments pass more detailed legislation than others; but in either case ministers are likely to provide yet more detailed directions for agencies. Some legislation actually *requires* ministers to provide directions, for example, the CSIS Act. The most detailed rules or ‘guidelines’ will be those developed with the agencies and are normally unpublished.

Clearly, the central institutions of control identified in the Figure also play a role in oversight. Indeed, in some parliamentary systems prior to intelligence reform, it was claimed that it was inherent in the constitutional process that there could be no independent oversight of security intelligence and that both control and oversight was provided by a single institution, usually a minister. This was certainly the case in the United Kingdom based on the doctrine of ‘ministerial responsibility’ to Parliament. Even though the inadequacy of this doctrine has now been acknowledged, we can see that agency directors, ministers, parliaments and some judges will exercise both functions. This is inevitable but only becomes a problem if there are no *additional* institutions of oversight with their own organisational basis.

Thus oversight institutions must also exist at each level, must report to those responsible for control at that level and will normally be located there (for example, agency, ministry, assembly). This location within agencies or ministries raises concerns as to the real extent of their independence but the danger of their being compromised can be reduced by securing their right to communicate with oversight bodies at other levels (see further below). Regarding ‘level’ one, it may seem odd to talk of oversight functions *within* agencies themselves but if oversight is *only* an external function then it becomes easier for agencies to see it as something troublesome that should be resisted. Instead, ideas of propriety must be internalised within the culture of agencies. However, although internal oversight is a necessary condition for public control, it is not sufficient: it must be backed up by external oversight at ‘levels’ two and three.

Oversight bodies are usually quite small with limited resources and their effectiveness can be enhanced in several ways. One way of seeking to protect their independence is to require them to copy reports to the oversight body at the next level. Depending on the precise institutional arrangements, this may be subject to some secrecy constraints but it will help to reduce the dependence of oversight on

the agencies themselves. So, for example, if an internal agency body such as an 'Office of Professional Responsibility' reports to the Agency Director on some matter the report should also be made available to whatever oversight institution exists within the ministry, for example, an inspector general. Similarly, reports from inspectors general to the minister should be made available to the review committee at 'level' three, whether it is a joint parliamentary committee such as in Brazil or the UK or a non-parliamentary body such as SIRC in Canada. If reports cross the secrecy barriers existing between the different levels of the state then how is appropriate security of information to be maintained? Ultimately this has to rely on consultation and trust between institutions at different levels and the discretion exercised by those involved. This is particularly the case for those working at 'level three' who, elected or not, must provide some accounting to citizens. Clearly these people cannot simply reveal all they know to the public (hence the diagonal 'secrecy' line in the Figure) but they must be prepared to challenge the fetish of secrecy and reveal what they discover unless it would clearly damage the security of the nation or the rights of individuals.

Secrecy is relevant to intelligence in two distinct forms: the first seeks to ensure that state officials will only have access to information if they have been cleared by security vetting for access at the appropriate level of *classification*. Normally, the higher an official is promoted or the nearer she is working to military or security matters, the higher the clearance she will need – for example, from 'confidential' to 'secret' to 'top secret'. Within the security intelligence sector the second dimension is *compartmentalisation*. Even though officials may be cleared to the highest level, it is still believed that the circulation of knowledge with respect to particular techniques, operations or targets should be minimised in the interests of security. Therefore individuals only have access to the information that they 'need to know'.

Now, these dimensions of secrecy have many implications. For example, they may hinder the efficacy of intelligence by reducing the flow of information both within agencies and, even more, between them. The failure of agencies to share information through some combination of proper concerns for security and petty bureaucratic jealousies is a common feature of intelligence 'systems' but there is insufficient space to consider this fully here (for a recently declassified CIA study of this problem, see Center for the Study of Intelligence, 1977). Clearly, secrecy presents a major hurdle to be surmounted if public control is to be achieved. The ability of outside bodies to oversee or review intelligence agencies depends on their

ability to obtain relevant information; if the agencies themselves will not provide it then those bodies are stymied because there will be little information available that is independent and useful. In most areas of state policy there is a broader 'policy community' of research organisations, 'think-tanks', lobbying groups, journalists and academics that can provide a source of information and ideas independent of the state but in the area of security intelligence it is only small. There have been numerous information and secrecy struggles between executive and oversight committees since 911, some of which are discussed below.

In general, it is most important that oversight institutions at different levels co-operate and help each other; this will not be without difficulties since the primary organisational loyalties of agency staff, inspectors general and parliamentarians are very different but without such co-operation, oversight will be fragmented and consequently less effective. This becomes increasingly important because of what might be called the 'decompartmentalisation' of intelligence. For example, in Europe (well before 911) a convergence of various issues was evident in what Bigo (1994) called the 'security continuum' (terrorism-drugs-'organised crime-illegal immigrants-asylum seekers). 911 has reinforced this and we see it in institutional form in the equal convergence of what used to be relatively distinct fields of intelligence: military, foreign, domestic/internal, law enforcement. If the control of intelligence networks is to be remotely effective then there must also be an oversight network.

Has 911 reversed the 1990s trend towards democratisation?

In order to provide an initial evaluation of the impact of September 11 2001 on the relative strengths of control and oversight, it is proposed to discuss briefly some of the actions taken by executives, oversight committees, courts and judges. Most of the examples are taken from Canada, the US and UK.

Control

Unsurprisingly, political executives responding to a perceived 'failure' on the scale of 911 will try to increase their capabilities both of a) action/power and b) information/intelligence. In the last year we can see changes made in each of the forms of control shown in the Figure. For example, new statutes have been passed: in Canada the Anti-Terrorism Act, in the US the PATRIOT Act and in the UK the Anti-

Terrorism, Crime and Security Act. Each of these extends the legal powers of governments to carry out surveillance and act against individuals and groups identified as terrorist or, especially in the case of the UK, engaged in other serious crime.

But it is not just legal rules that have been re-written; probably the most dramatic assertions of power have been those in the military field, especially the extension of the traditional right of national self-defence to encompass pre-emptive attacks but these are beyond the scope of this paper. In the wake of the intelligence scandals and inquiries of the 1970s the US Congress sought to restrict the autonomy of the intelligence agencies (e.g. see Johnson, 1985; Olmsted, 1996). Many of these restrictions are now being modified if not abandoned. For example, questions have been raised concerning the extent to which the expansion of US Special Forces operations overseas has been consistent with the requirement for prior notice being given to the Intelligence Committees (NYT Aug 12, 2002). Another restriction was the erection of a 'firewall' between information generated for intelligence purposes and that used for the purposes of law enforcement evidence. Since the 1970s the increasing co-operation between military, intelligence and law enforcement agencies in the targeting of organised crime and the increased use of tactics of disruption (rather than arrest and prosecution) had already put pressure on this division. In the wake of 911 that pressure has increased tremendously: this can be seen clearly from the dispute over the use to be made of information obtained through wiretaps authorised by the special court established by the Foreign Intelligence Surveillance Act (FISA). After a series of court decisions the special appellate panel of the Foreign Intelligence Court of Review upheld the PATRIOT Act's grant of increased powers so that prosecutors would be permitted to use information obtained from FISA authorised interceptions in the prosecution of those accused of terrorism (NYT Aug 1, 2002; NYT Nov 24, 2002). Ironically, this decision came shortly after it was revealed by the Senate Judiciary Committee that in 75 warrant applications, mainly during the Clinton administration, the FBI and Justice Department had misled the FISA as to the actual existence of the 'firewall': information gathered from intelligence taps was used freely in bringing criminal charges (NYT Aug 23, 2002).

In the US itself a major manifestation of the Presidential need to be seen to be in control is visible in the plans to re-organise security intelligence structures. Legislation has been passed to create a new Department of Homeland Security (DHS). This proposal seems to have been guided by two main arguments: first, that

the ‘failure’ of 911 was largely a failure to co-ordinate intelligence and security and, second, that a grand political gesture was required to convince the US public that ‘something is being done’ to improve security. Thus the plan is based on the strategy of combining previously disparate security organisations in the apparent belief that improved hierarchical co-ordination will improve matters. This strategy might well be criticised (for example, hierarchical forms of organisation are infamously poor at effectively developing and disseminating accurate information) but the main opposition to the plan in Congress was less about its wisdom *per se* than directed towards accompanying Presidential assertions of power. For example, the executive wanted to exempt the DHS both from access to information rules with respect to ‘critical infrastructure’ information (WP July 17, 2002; see also WP Feb 24, 2002) and from whistleblower protection (NYT June 27, 2002). Consistent with an earlier Presidential order barring unionisation for over 500 employees in parts of Justice Department (NYT Jan 16, 2002), DHS employees will enjoy fewer employment rights than elsewhere in the federal government (WP Nov 21 2002).

It remains to be seen whether the DHS will succeed in its aim of co-ordinating domestic security programmes. The original White House proposal did not give much prominence to intelligence co-ordination. Finally the Act establishes a division for ‘Information Analysis and Infrastructure Protection’. Its analyses and warnings will be developed from a combination of product passed by CIA, FBI etc. and information gathered by, for example, border guards and secret service who are to be brought into the department (WP July 18 2002; NYT Nov 20 2002). It is hard to see how this will achieve any co-ordination of security intelligence in the notoriously fragmented US ‘community’. The most likely future scenario is of competing analytical centres with the presidency left to pick out the preferred intelligence (e.g. FAS, Sept 9, 2002).

There are already signs of a politicisation of analysis in the reports that the Pentagon has established a new analytical branch with the task of re-sifting information in the search for the elusive ‘intelligence’ proving a link between the 911 attacks and Iraq after the failure of CIA analysts to do so (*Guardian*, October 9, 10; NYT Nov 3 2002). More generally, the Pentagon is reportedly developing the infrastructure for increased covert operations (LAT Oct 27 2002).

The FBI remains outside the DHS apart from its critical infrastructure component that will be transferred. But the FBI itself has not escaped from re-organisation efforts: CIA personnel were deployed to advise the Bureau on establishing its Office of

Intelligence (Mueller, 2002). However this and increasing the proportion of agents working on counter-terrorism have not satisfied all that the Bureau can transform itself from a law enforcement into domestic security intelligence agency. There is clearly a debate underway in Washington DC as to whether the US should separate the two functions as Canada did in 1984 and as characterises the separation of police and security service in the UK (e.g. see WP, Nov 16 2002).

Of course, if executives are to deploy their new powers effectively then they depend on intelligence: some highly significant shifts have been made in the attempt to increase both the quantity and the quality of intelligence developed with respect to 'terrorism'. This is hardly surprising but does reflect serious distortions in the understanding of just what kind of failure 911 represented. Arguably too much of the congressional and media discussion since 911 has centred on the search for pieces of information that would, it is assumed, have enabled the 911 attacks to be predicted and then prevented. If not the search for the 'smoking gun' then perhaps the search for the 'smouldering datum'! Given what is known about the *modus operandi* of those carrying out the attacks, it is extremely unlikely that such a piece of information exists. Nor was it just a case of the system failing 'to join the dots' between pieces of data so that warning could have been provided though this starts to get closer to the real failure of US intelligence: the failure of processing and analysis (e.g. Whitaker, 2002).

Analysts have always been the poor relations of gatherers within intelligence communities: they enjoy neither the reputation for 'derring-do' associated with HUMINT nor the capacity to generate large profits for equipment suppliers associated with TECHINT. Certainly there *were* failures in gathering prior to 911, for example, the failure of FBI and CIA (Baer 2002) to develop human sources home and abroad. But the US intelligence 'community' was already awash with data and it is far from clear that increasing the flow further will enhance the ability to prevent further 'failures'.

There are numerous examples of this desire to increase the gathering of information reflected in changes in the law or, in some cases, executive assertions that previous law does not apply. The clearest example of the latter is detention without trial, both of two US citizens and 1200 non-citizens (NYT June 23, 2002; HRW Aug 15, 2002). The clear purpose of this is to gather information; whether people are ever placed on trial is a subsidiary consideration. The desire to gather information has led not only to

US agencies co-operating abroad with agencies long associated with human rights abuses, e.g. Pakistan (LAT Aug 25, 2000) but also transferring individuals arrested in one country to another 'that is able to extract information from them' for passing on to the US (WP Nov 1 2002). Transnational information exchange is one thing, brokering the use of torture is another.

Regarding TECHINT, in both the US and Europe executives are seeking improved access to electronic data. For example, the European Union has amended its 1997 Directive on Privacy so that obligation of communications service providers to erase traffic data is deleted and so that they retain data for 12-24 months (Statewatch 12(3-4) 2002, 1). The EU and USA are also discussing an information exchange agreement between Europol and US agencies that appears unlikely to include the normal EU data protection provisions (Statewatch, Nov 29 2002, press release).

As well as executive assertions of power both to act and gather information, there have been significant struggles over 'information control' between executive (and agencies) and oversight bodies. The notion of 'executive privilege' in the US and the UK Official Secrets Acts are all premised on the belief that executives should be sole determinants of what security information, if any, is passed to assemblies. For example, the UK Intelligence Services Act 1994 states explicitly that the 'gatekeeper' for information made available to the Parliamentary Intelligence and Security Committee is the Minister (cf. Gill, 1996).

In general, the more counter-terrorism is viewed as 'war' then the greater the emphasis given by executives to 'secrecy' (both as counter-intelligence and as an essential prerequisite for 'surprising' enemies). There are several areas in which the US executive has sought to reduce the flow of information: in a memo to federal agencies Attorney General Ashcroft encouraged resistance to freedom of information requests – not in relation to security but more broadly in relation to 'institutional, commercial and personal privacy interests (SFC Jan 6, 2002, *Guardian* Mar 6, 2002). The Congressional Judiciary Committees criticised the Justice Department for seeking to deny information regarding its counter-terrorism policies under PATRIOT Act (WP Aug 21, 2002).

The Joint Inquiry into 911 established by the two intelligence committees has also been critical of attempts by the Executive to deny them access to information, for example, the refusal by the FBI to make available for testimony an informer and his

handler (NYT Oct 6 2002) and that of the Director of Central Intelligence to declassify references to the Intelligence Community providing information to the White House (Hill, 2002). For those more familiar with Parliamentary regimes, this denial is probably less surprising. For example, in the Canadian Security Intelligence Service Act 1984 Cabinet documents are explicitly excluded from the general rule that SIRC has access to all information (CSIS Act s.39).

In the struggle for information control in the US the executive has also complained about the leaking of information from House and Senate Intelligence Committees regarding NSA interception of two 'warning' messages on Sept 10 2001 that were not translated until Sept. 12. In the face of these complaints, the committee chairs requested a FBI investigation of the leaks (WP, June 21, 2002). Thus the answer to the question 'who guards the guards who guard the guards' is….'the guards'! It is to the impact of 911 on oversight that we turn now.

Oversight

Oversight is an extremely difficult task to perform in the security intelligence area if for no other reason than the all-pervading secrecy (see above). The normal dependence of overseers for information on the agencies themselves may result in the undermining of the whole process. The example of the FBI misleading the FISA court was given above. Another interesting insight into the problems here was provided by *Guardian* journalist, Martin Bright who appeared before the UK Special Immigration Appeals Commission that hears challenges to minister's decisions on detention and deportation on security grounds. He described the types of information presented by the agencies: a small number of government documents including intelligence, court documents from trials and press cuttings. Since the last of these are often based on secret briefings by intelligence officers to grateful journalists, their production as independent 'evidence' is misleading, to put it mildly (*Observer* July 21, 2002).

The pressure on overseers generally to 'look the other way' is likely to increase following failures such as 911 and nowhere will this be greater than at levels one and two (see Figure) where there will be enormous political pressure on the ministries and agencies to deliver. Little has emerged of how these 'internal' oversight bodies have been performing since 911 but one example is that of the Office of Inspector General in the Justice Department investigating 9 allegations of excessive force,

illegal detention etc. under PATRIOT Act that was to present a report to Congress in October on treatment of 911 detainees (FAS, July 16, 2002).

'Internal' oversight at levels one and two is very important- without it those working inside the system may more easily regard oversight as simply the product of meddlesome outsiders that should be resisted – but that at level three is the most crucial if public confidence in the security intelligence agencies is to be maintained. Here, the most systematic review or oversight is likely to be provided by specialist committees either *inside* national legislatures, for example, the Intelligence Committees of the US Senate and House of Representatives (for overview see Holt, 2000) and the joint committees made up of members of both houses in the UK and Brazilian Parliaments or *outside* such as SIRC in Canada and the Committee for Monitoring of Intelligence, Surveillance and Security Services in Norway. The other potential oversight institution at this level is judges who, in some countries, are involved in the authorisation of warrants for intrusive surveillance (in terms of the earlier discussion of terminology this role involves elements both of control and oversight). Also, more episodic review may be provided by courts.

Legislative and Other Committees

In the US the primary effort of the congressional committees has been its investigation of the 911 'failure'. For example, a report of the Subcommittee on Terrorism of the House Intelligence Committee noted the lack of HUMINT in CIA and poor dissemination to other agencies; that FBI counter-terrorism was hindered by decentralisation and the culture of 'crime-fighting'; and that the NSA needing to be more proactive in gathering (STHS, 2002). The major congressional effort in the year following September 11 was a joint inquiry by the two Intelligence Committees. This identified seven areas of investigation including: evolution of the terrorist threat to US and the Government's response; what the Intelligence Community (defined as 14 agencies) knew prior to 911; what the Intelligence Community has learnt since 911 about perpetrators and clues to explaining the failure; what has emerged about systemic problems impeding the Community; how the Intelligence Community interacts with each other and the rest of the Government in countering terrorism. The overall interim conclusion was that:

> *the Intelligence Community did have general indications of a possible terrorist attack against the US or US interests overseas in the spring and summer of*

> *2001 and promulgated strategic warnings. However, it does not appear to date that the Intelligence Community had information prior to September 11 that identified precisely where, when and how the attacks were to be carried out.* (Hill, 2002)

The concern of senior members of the inquiry at what they described as inadequate co-operation from the executive branch led them to endorse the idea that a separate commission of inquiry into 911 should be established (FAS, Sept 19 2002). This idea had been growing in strength for some months, was supported by the families of victims of 911 and the House of Representatives had voted to support the idea in July. The White House had opposed the move, saying it would distract the agencies from their primary tasks but on September 20 signalled it would abandon its opposition (NYT Sept 21 2002). However, it was only after further wrangling between White House and Congress that agreement was reached in the last session before Congress adjourned for the year (NYT Nov 15 2002) and the 10 member Commission, required to complete its work within 18 months, is to be headed by Henry Kissinger (NYT Nov 28 2002).

In Canada the main burden of oversight at this level is the responsibility of the Security Intelligence Review Committee (SIRC). Members (there are currently three but may be up to five) are appointed by the PM and serve part time. SIRC has a full-time staff of 16 and two main functions: to review the activities of CSIS and investigate complaints about the Service. The Committee may also hold hearings on challenges to CSIS security assessments. Overall, SIRC regards its role as reviewing whether CSIS 'has acted appropriately and within the law' (SIRC, 2002, 3). Building on previous reviews of CSIS' counter-terrorism work, SIRC established the following objectives for its study: 'the reach and focus' of CSIS investigation of Sunni Islamic extremist activities; the 'nature and quantity of assessments, analyses' and other advice disseminated to government and law enforcement; and the 'character and quantity of information exchanges' with allied services (SIRC, 2002, 5). SIRC made no claim that its review was comprehensive, saying that it concentrated on how the Service ran its investigation, its analytical outcomes and the advice disseminated to government. Its conclusion was very similar to that of the US Joint Inquiry Staff Report quoted above:

> *Although none of the intelligence products or threat warnings we reviewed pointed directly to the events of September 11, the Service clearly was aware*

> *of the potential for Al Qaida-inspired terrorist attacks of some kind and communicated this information to the appropriate bodies in government. In the Committee's view, however, none of the advice or communications the Committee reviewed warned of a threat sufficiently specific in time or place to have alerted government authorities to the events of September 11.* (SIRC, 2002, 7)

By comparison with the extensive external inquiries in the US and even the more modest SIRC enquiry, that in the UK has been minuscule. The Annual Report of the Intelligence and Security Committee (I&SC, 2002) identified some resource pressures in the Security Service, Secret Intelligence Service and Defence Intelligence Staff (para 61), referred to a Joint Intelligence Committee July 2001 assessment that al-Qaeda attacks were in the final planning stages but that timings, targets and methods were unknown (para.65); noted the re-deployment of staff post-911 (paras. 67-9) and the increased Security Service resources in collection and dissemination (para. 72) but, significantly, said nothing about analytical deficiencies. Finally, it noted the lack of linguists (para. 77).

Comparing these three reports, it is noticeable that they are all entirely concerned with issue of 'efficacy' – was there anything that the agencies could have done to prevent the September 11 attacks? The only acknowledgement of propriety issues is the SIRC comment that their review did not examine the compliance with law and policy of CSIS warrants and handling of human sources (SIRC, 2002, 5). It is also important to note the significant methodological differences between these reviews, largely but not entirely determined by the availability of staff. The US Joint Inquiry team had 24 researchers divided into five investigative teams that interviewed officials, reviewed documents and submitted questionnaires not only at the FBI, CIA and NSA but also other departments (Hill, 2002). We might assume that about ten of SIRC's staff at most would have been involved in its 911 inquiry and they made no claim to have examined 'all the raw intelligence' available to CSIS (SIRC, 2002, 5). But these staff would also have carried out interviews and reviewed documents. The UK effort, by comparison, was hampered from the start by the fact that half of the nine-person committee (including the Chair) was newly appointed after the 2001 election. The members themselves 'took evidence' over the year from 37 witnesses (ministers, heads of services and other officials) and made 'visits' to the agencies. But what might properly be described as 'investigative' work fell to the single investigator who was tasked to carry out five investigations during the year none of

which appear to have concerned 911 (I&SC, 2002, 5, 29-31). The conclusions drawn by the I&SC appear to have been based entirely on briefings from agency heads; at least, there is nothing in the Report to lead one to suppose otherwise.

Courts and Judges

It is in the US where security intelligence issues are most likely to end up in court, though even here, special arrangements have been made to hear some cases, e.g., FISA courts. But the Bill of Rights remains a fertile field within which lawyers have sought to test the constitutionality of some of the executive and legislative measures taken since 911. For example, federal judges in various parts of the country have ordered an end to secret deportation hearings, have tried to limit the executive's use of the material witness law to sustain unlimited detention and have ordered the executive to publish the names of the 1200 people detained after 911 (LAT Aug 6, 2002). A federal judge in LA ruled as unconstitutional a 1996 law making it a crime to provide 'material support' to any foreign organisation deemed by State Department as 'terrorist' on the grounds that groups have no chance to defend themselves (NYT June 24, 2002) but prosecutors continue to use the law pending appeals (WP Oct 15 2002).

In the UK one of the most controversial elements of the Anti-Terrorism, Crime and Security Act was that it empowered the Government to detain without trial non-citizens who the Government could not deport because of fears for their safety in their home country. The Special Immigration Appeals Committee ruled this to be discriminatory and therefore contrary to the Human Rights Act 1998 because it applied only to non-British citizens (*Guardian* July 31, 2002). However, this decision was reversed subsequently in the Court of Appeal.

Finally, what examples have there been of 'oversight' taking place at level four? First, a number of the cases reported above have been challenges supported by civil liberty groups such as the American Civil Liberties Union who have filed 24 relevant lawsuits since 911 (Wired News, Oct 16 2002) and Liberty in the UK. Second, there have been efforts at more wide-ranging critiques of executive initiatives: for example, Electronic Privacy Information Center (EPIC) and Privacy International produced a joint report regarding the impact of current and proposed laws in 50 countries since 911. It identifies four main trends: swift erosion of pro-privacy laws (as in the EU example above); greater data sharing between corporations, police and security

agencies; greater eavesdropping (see above); and, sharply increased interest in people-tracking technologies (CNET Sept 3, 2002).

Conclusion

What are the lessons for the future of the control and oversight of intelligence of this necessarily brief review of some developments in the last year? Clearly, the impact of September 2001 is still working through intelligence and governmental systems across the world and will do so for the foreseeable future. It is not possible to predict the direction of these changes especially given the essential uncertainties surrounding the outcome of an US-led attack on Iraq and of further attacks by al-Qaeda. But if much has changed in the security intelligence world in the past year, it is still important to maintain a grasp of some hard-learned lessons so that the democratic gains of the 1990s are not squandered in a security panic in the 2000s.

First, we should not accept the 'balance' metaphor: rights relating to privacy, speech etc. cannot simply be weighed against security factors. Limitations on rights can only be justified in terms of proportionality to the nature and size of the security threat (cf. Lustgarten & Leigh, 1994). Reductions in rights and freedoms do not make for greater security, they make for less democratic societies in which the possibilities of abuse and harm by the state or vengeful populations are increased.

Second, (often very small) oversight bodies at different levels must co-operate with each other, including sharing information wherever possible subject to minimal necessary secrecy requirements. The trap to be avoided is that oversight itself becomes compartmentalised as it is in the UK where the Government still denies the Parliamentary Committee access to the confidential annexes of reports made by the judicial commissioners regarding interception warrants (PM, 2002, para. 23). Though the term intelligence 'community' often attracts hollow laughter because of the inter-agency conflicts and 'turf wars' that take place, we must acknowledge that ever-increasing sharing of information is occurring both within and between public and private intelligence sectors. This is clearly necessary in the interests of efficacy but also raises higher the potential risks of abuse, for example, by the sub-contracting of operations to agencies less imbued with a culture of human rights. Oversight bodies, both within particular countries, and in different countries must seek to assist each other; what is needed is an oversight community.

In the post-911 environment it is natural that oversight bodies have been primarily concerned with their agencies' effectiveness and, as we have argued, this is entirely in keeping with overall democratic control of intelligence. But it is important that they beware incorporation by agencies into management rather than oversight tasks. All oversight bodies owe important duties to uphold human rights and liberties and thus their engagement with the agencies must always retain a critical and sceptical approach without which they may be reduced to the role of mere management consultants.

References

Abbreviated references in the text are to the following media sources:

FAS: Federation of American Scientists, *Secrecy News*
LAT: *Los Angeles Times*
NYT: *New York Times*
SFC: *San Francisco Chronicle*
WP: *Washington Post*

Baer R. (2002) *See No Evil*, New York: Crown Publishers.

Bigo D. (1994) 'The European internal security field: stakes and rivalries in a newly developing area of police intervention,' in M. Anderson & M den Boer (eds.) *Policing Across National Boundaries*, London: Pinter Publishers.

Caparini M. (2002) 'Challenges of Control and Oversight of Intelligence Services in a Liberal Democracy,' Paper presented to *Workshop on Democratic and Parliamentary Oversight of Intelligence Services*, Centre for the Democratic Control of Armed Force, Geneva, October.

Center for the Study of Intelligence (1977) 'Critique of the Codeword Compartment in the CIA,' Central Intelligence Agency, March, accessed at www.fas.org/sgp/othergov/codeword.html

Cepik A. and Antunes P. (2001) 'The New Brazilian Intelligence Law: an institutional assessment,' Paper given to Center for Hemispheric Defense Studies, Washington DC,May.

Edelman M. (1964) *The Symbolic Uses of Politics*, Illinois: University of Illinois Press.

Gill P. (1994) *Policing Politics: security intelligence and the liberal democratic state*, London: Cass.

Gill P. (1996) 'Reasserting Control: recent changes in the oversight of the UK Intelligence community,' *Intelligence and National Security*, 11(2), pp. 313-31.

Giménez-Salinas A. (2002) 'The Spanish Intelligence Services,' in J.-P. Brodeur *et al* (eds.) *Democracy, Law and Security: internal security services in contemporary Europe*, Alershot: Ashgate.

Hastedt G.P. (1991) 'Towards the Comparative Study of Intelligence,' *Conflict Quarterly*, XI:3, 55-72.

Hill E. (2002) Joint Inquiry Staff Statement, Part I, House Permanent Select Committee on Intelligence and Senate Select Committee on Intelligence, September 18, www.fas.org/irp/congress/2002_hr/091802hill.html

Holt P.M. (2000) 'Who's Watching the Store? Executive-Branch and Congressional Surveillance,' in C. Eisendrath (ed.) *National Insecurity: US Intelligence after the Cold War*, Philadelphia: Temple University Press.

I&SC (002) *Annual Report 2001-2002*, Intelligence and Security Committee, Cm 5542, June.

Joffe A.H. (1999) 'Dismantling Intelligence Agencies,' *Crime, Law & Social Change* 32: 325-46.

Johnson L.K. (1985) *A Season of Inquiry: the Senate intelligence investigation*, Lexington: University Press of Kentucky.

Lustgarten L. & Leigh I. (1994) *In From the Cold: national security and parliamentary democracy*, Oxford: Clarendon Press.

McDonald D. (1981) *Commission of Enquiry Concerning Certain Activities of the RCMP*, Three Reports (First published 1979), Ottawa: Minister of Supply and Services.

Mueller R. (2002) Testimony of Robert S. Mueller III, Director FBI, before the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence, October 17.

Olmsted K.S. (1996) *Challenging the Secret Government: the post-Watergate investigations of the CIA and FBI*, Chapel Hill: University of North Carolina Press.

PM (2002) *Government Response to the Intelligence and Security Committee's Annual Report 2001-2002*, Presented to Parliament by the Prime Minister, June.

Rzeplinski A. (2002) 'Security Services in Poland and their Oversight,' in J.-P. Brodeur *et al* (eds.) *Democracy, Law and Security: internal security services in contemporary Europe*, Aldershot: Ashgate.

SIRC (2002) *Report 2001-2002: an operational audit of the Canadian Security Intelligence Service*, Ottawa: Public Works and Government Services Canada.

STHS (2002) 'Counterterrorism Intelligence Capabilities and Performance Prior to 9-11,' Report of the Subcommittee on Terrorism and Homeland Security of the House Permanent Select Committee on Intelligence, July.

Szikinger I. (2002) 'National Security in Hungary,' in J.-P. Brodeur *et al* (eds.) *Democracy, Law and Security: internal security services in contemporary Europe*, Aldershot: Ashgate.

Whitaker R. (2002) 'A Poor Bargain,' *New Scientist* 174, June 29, p.26.

Established in 2000 on the initiative of the Swiss government, the Geneva Centre for the Democratic Control of Armed Forces (DCAF) encourages and supports States and non-State governed institutions in their efforts to strengthen democratic and civilian control of armed and security forces, and promotes international cooperation within this field, initially targeting Euro-Atlantic regions.

The Centre collects information, undertakes research and engages in networking activities in order to identify problems, to establish lessons learned and to propose the best practices in the field of democratic control of armed forces and civil-military relations. The Centre provides its expertise and support to all interested parties, in particular governments, parliaments, military authorities, international organisations, non-governmental organisations, academic circles.

Geneva Centre for the Democratic Control of Armed Forces (DCAF):
rue de Chantepoulet 11, P.O.Box 1360, CH-1211 Geneva 1, Switzerland
Tel: ++41 22 741 77 00; Fax: ++41 22 741 77 05
E-mail: info@dcaf.ch
Website: http://www.dcaf.ch