Obstacles to the Oversight of the UK Intelligence Community

https://www.e-ir.info/2013/07/19/obstacles-to-the-oversight-of-the-uk-intelligence-community/

PETER GILL, JUL 19 2013

Oversight and its Challenges

Effective oversight of state intelligence activities matters: agencies exist to protect public safety and security but they possess special powers to infringe on privacy and, if unchecked, their actions may be highly damaging to democratic rights. Currently there is much discussion in the UK of Edward Snowden's revelations of the extensive surveillance of communications by the US National Security Agency (NSA) and UK Government Communications Headquarters (GCHQ) which illustrates the shortcomings of the current system of oversight.[1]

What exactly do we mean by 'oversight' and how is it different from the 'control' or management of agencies? 'Oversight' refers to the review or scrutiny of intelligence activities so that those directing them can be held accountable. The main objective of the scrutiny is to secure public trust in the agencies through ensuring that their expenditure is efficient and effective and that their operations are legal with proper respect for human rights. This scrutiny will, ideally, be carried out both by specialist units *within* agencies and ministries as well as externally by parliamentary and/or extra-parliamentary bodies.

There are particular problems inherent in intelligence oversight everywhere. Foremost is the secrecy within which intelligence operates. In some respects there is more openness now about intelligence than there was during the Cold War; for example, UK governments denied the very existence of MI6 in peacetime and until the 1980s there simply was no external oversight of intelligence in the UK. Yet the agencies are especially concerned to safeguard their 'sources and methods' for fear that, if they are revealed, operations will be compromised and, in the case of human sources, possibly killed. But while this secrecy is justified, it can facilitate abuse of power, inefficiency or corruption. Second, matters of national security and public safety are the central concern of any democratic government and consequently intelligence agencies are close to the heart of political power. This brings an ever-present danger of intelligence being politicised; rather than 'speaking truth unto power', agencies may tell politicians what they wish to hear or act in their partisan interest by surveilling opponents.[2]

Intelligence Oversight in the UK

The most public part of the UK oversight architecture is the Intelligence and Security Committee (ISC)[3] which was established as a 'committee of parliamentarians' in 1994. It had the same mandate as a departmental select committee – to review the expenditure, administration and policy of the Agencies – but its reporting and appointments process differed, for example, its members were selected by and it reported to the Prime Minister who would subsequently lay their report before Parliament, having 'redacted' any material potentially damaging to security. Since its inception the role of the ISC has developed mainly at the committee's own instigation but also reinforced by legislation. ISC quickly extended its review from the three core intelligence agencies, MI5, MI6 and GCHQ, to include the Defence Intelligence Staff and national law enforcement intelligence and, in 2012, the government largely accepted the committee's own recommendations that it should become a statutory committee of Parliament with a greater degree of independence and increased access to information. Some of these changes are mainly symbolic, for example, it has only cited one case in which it has been prevented from accessing information it asked for, but

much will depend on whether the government honours its commitment to provide the committee with more resources (*Annual Report for 2012-13*, 42-43).

In the UK, as elsewhere, a parliamentary committee is a necessary condition for effective and efficient oversight because of Parliament's function to check the Executive, including controlling state budgets and holding officials to account. Parliament also has a key role in public education; this is especially important regarding intelligence since people may know little yet suspect much because secrecy was formerly total. But it is not sufficient because MPs are very busy people and, so far, ISC has had little or no research staff. Most of the evidence taken by ISC has been in the form of briefings by agency heads and other senior officials or as written responses. This is inadequate for credible and effective oversight: comparing ISC's two investigations into the 7/7 London bombings demonstrates the importance of having access to primary materials. Its first report (May 2006, Cm6785) was based essentially on briefings from senior officials which, as it turned out, failed to tell the whole story but their much fuller second report (May 2009, Cm7617) was based on closer examination of relevant surveillance materials.[4] It is generally argued that outsiders require 12 to 18 months to get to grips with understanding the somewhat arcane world of intelligence; accordingly some kind of full time research capability is essential.

ISC is complemented by three judicial commissioners. An Interception of Communications Commissioner (ICC)[5] reviews the warrant issuing process, ministers' and agencies' performance in acquiring and disclosing communications data and the process by which agencies other than intelligence and military gain access to encrypted data. An Intelligence Services Commissioner[6] (ISCommr.) reviews the authorisation of 'interference with property', electronic surveillance, 'covert human intelligence sources' (CHIS) and the requirement that Communication Service Providers (CSPs) disclose encrypted data. A Surveillance Commissioner[7] oversees surveillance by police and other public bodies, other than communications interception which is covered by ICC. All these commissioners now provide annual reports in which they describe their inspections process but the concentration is still on their relatively narrow mandate of checking that the authorisation process has been followed correctly. The ISCommr has been given the additional task of checking on compliance by UK intelligence and military officers with the new Guidance on the interrogation of detainees[8] issued by government in the wake of the scandal around UK collusion in the kidnapping and torture (aka 'extraordinary rendition') of alleged terrorists.[9]

Communications Surveillance

But we have learnt of highly controversial policies such as rendition and mass communications surveillance not from these formal institutional mechanisms of oversight in UK; rather, they have come as a result of whistleblowers, legal actions and investigative journalism. From ICC Reports we are familiar with the targeted interception and the collection of communications data (CD)[10] on the basis of warrants and/or requests to CSPs based on a known framework of law and oversight. Ministers sign warrants for the interception of mail, telephone, e-mail, mobile phones, computers and so on in order to obtain the content of a communication. Warrants have to identify the necessity and proportionality of interception in order to remain compliant with the Human Rights Act. The agencies do not require a warrant in order to collect the metadata that they use to locate people and their networks.

In the context of the UK Government publishing a draft Communications Data Bill in June 2012 that was intended to up-date powers to intercept communications to the age of social networks and Skype, the ISC inquired into the specific impact on the security and intelligence agencies, publishing its report in February 2013. The report is interesting as to the existence of the gap in the 'capability' of agencies to access CD, and how the government could require, if appropriately authorised, CSPs to apply Deep Packet Inspection probes into their networks to collect the required information. However, there was no mention of the mass collection of data for the purposes of data mining, for which the legal basis is contested and oversight non-existent. Nor was there in the ICC's report for 2011.[11]

This is potentially far more invasive of privacy rights than targeted interceptions in accordance with law. It has been evident for the past decade that the 'big idea' in security and technology post-9/11 has been the promise of 'joining the dots' through the analysis of massive data warehouses combining both public (employment, health, education…) and private (finance, travel, insurance…) data. Identifying and locating targets for surveillance is the first problem for intelligence agencies and, beyond the traditional methods of informers and contacts of those already known, the new

communications technologies seemed to hold out the prospect of identifying those currently 'unknown'. Based on some 'profile' of suspicious behaviour, travel or financial pattern, data banks would be searched for names, numbers etc. that required further checking. We already knew from the reports of the Echelon system in the 1990s that transatlantic satellite communications would be searched by means of a 'dictionary' of keywords so that the messages containing them could be further interrogated.[12]

Snowden has now provided much information to fill the gaps on the mechanics of this surveillance. Clearly, the communications infrastructure is in largely private hands and the cost of interception are much reduced if the CSPs cooperate. They are required by law to cooperate with specific targeted warrants but what of mass data collection of communications involving not just those already targeted but more speculative data mining? Apparently the NSA's PRISM programme relies on collecting directly from the servers of providers such as Microsoft, Google and Facebook. However, not all CSPs cooperate in this way and there is a second programme – 'Upstream' – for the collection of data directly from fibre cables or infrastructure. NSA has been constructing a new facility in Utah for the storage and analysis of everything collected.[13] GCHQ also collects material from the cables as they come ashore from the Atlantic in an operation named Tempora.[14] If the material is kept for some time (permanently in the case of Utah) or from some years (as the EU has been seeking to have CSPs do on behalf of governments) then it is available for more thorough investigation.[15]

ISC and the ICC may well protest that their failure to discuss data mining was to preserve the integrity of intelligence methods but there has been enough discussion of the issue pre-Snowden that some official contribution would have been appropriate to educate and reassure (or not) the public. The ISC's one-line dismissal of GCHQ data mining via PRISM is clearly inadequate and did not even refer to their own 'Tempora' programme.[16]

Conclusion

What this makes clear is that oversight is insufficient, first, because of the inadequate legal basis for the authorisation and control of UK intelligence agencies and, second, institutions of oversight are overly-concerned with the legalities of intelligence practices compared with broader issues of ethics and public education. Effective oversight will always depend partly on an informal network of researchers, journalists and lawyers in civil society but a mature democracy must develop an oversight system with adequate powers and full-time research staff.

—

Peter Gill *is Honorary Senior Research Fellow at the University of Liverpool, UK. He is the author of Policing Politics (Cass 1994), Rounding Up the Usual Suspects? (Ashgate, 2000) and co-author of Intelligence in an Insecure World (2nd edn., Cambridge: Polity, 2012).*

[1] There might be even more discussion had most of the UK media followed up the Guardian's disclosures rather than acceding to a Defence Advisory notice from the Government asking them not to do so. See http://www.dnotice.org.uk/. References to the NSA files published in the UK since June 6 2013 by *The Guardian* can be found at http://www.guardian.co.uk/world/the-nsa-files?INTCMP=SRCH

[2] The issue of democratic control is discussed more fully in Peter Gill & Mark Phythian,*Intelligence in an Insecure World*, Cambridge: Polity, 2012, chapter 8.

[3] http://isc.independent.gov.uk/ is the ISC's web-site where copies of its reports can be found.

[4] Michael Mates, speaking on *Newsnight*, BBC2, May 19, 2009.

[5] http://www.iocco-uk.info/

[6] http://isc.intelligencecommissioners.com/docs/0497.pdf

[7] http://surveillancecommissioners.independent.gov.uk/

[8] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62632/Consolidated_Guidance_November_2011.pdf

[9] Ian Cobain, *Cruel Britannia: a secret history of torture*, London: Portobello Books, 2012

[10] Otherwise known as meta-data this is information relating to origin, destination, duration and location of calls but not the content. There is an argument that it is now impossible to collect one without the other.

[11] HC 496, July 2012 http://www.official-documents.gov.uk/document/hc1213/hc04/0496/0496.pdf

[12] Patrick Radden Keefe, *Chatter*, New York: Random House, 2006.

[13] James Bamford, 'The NSA is Building the Country's Biggest Spy Center (Watch What You Say)' http://www.wired.com/threatlevel/ March 15, 2012 Accessed July 7, 2013.

[14] http://www.guardian.co.uk/world/the-nsa-files?INTCMP=SRCH See articles dated June 21, 2013.

[15] There is the further problem of decrypting the highly sophisticated encryption now widely used. There is insufficient space here to deal with this but, for example, see Bamford, ibid.

[16] http://isc.independent.gov.uk/news-archive/17july2013

About the author:

Peter Gill is Honorary Senior Research Fellow at the University of Liverpool, UK. He is the author of Policing Politics (Cass 1994), Rounding Up the Usual Suspects? (Ashgate, 2000) and co-author of Intelligence in an Insecure World (2nd edn., Cambridge: Polity, 2012).