INTELLIGENCE AND NATIONAL SECURITY
https://doi.org/10.1080/02684527.2020.1783875

Routledge
Taylor & Francis Group

ARTICLE

Check for updates

Of intelligence oversight and the challenge of surveillance corporatism

Peter Gill

ABSTRACT

This article examines the experience of oversight during the last fifty years in order to inform current debates in both the older and newer democracies. First, there is a discussion of certain key concepts: intelligence governance including control, authorisation and oversight; second, the difficulties facing oversight, specifically, how these can be alleviated by a structure involving both parliamentary and specialist bodies and, third, the challenges presented by the structures of surveillance corporatism and its reliance on bulk collection. It is concluded that this new intelligence architecture requires a form of decentred regulation of and by state and corporate actors.

Introduction

Limited debate and reform on the issue of governing intelligence took place in the 1950s in some of the European democracies which had suffered most under Nazi rule, notably the Netherlands and West Germany, but barely surfaced elsewhere. In the 1970s and 1980s debate around issues of intelligence and, more broadly, surveillance, gathered pace, first, in North America and Australasia as scandals erupted and, second, in western Europe, less because of scandal and more because of the developing jurisprudence of the European Court of Human Rights. Debate more widely through Europe emerged in the 1990s once the Cold War ended and in Latin America with the demise of several military dictatorships.

Consequently, much progress has been made in improving the governance of intelligence in democratic regimes – both old and new – since the 1970s, though progress is not always as great in real terms as the passage of legislation and establishment of parliamentary committees might suggest. This article examines the experience of oversight during the last fifty years in order to inform current debates in both the older and newer democracies. National oversight practices vary quite widely and there is no attempt here to evaluate specific national systems but, rather, to draw more general conclusions. While it may not be possible to develop a universally valid theory of intelligence oversight because of the extremely wide variation of political cultures and practices, it is possible to move toward a normative theory of democratic oversight. It is important to note, however, that oversight is present in almost all authoritarian intelligence systems, carried out by a military junta, religious leadership or ruling party; if there is literally no oversight then any security and intelligence agency can truly be described as a 'state within a state'.

First, there is a discussion of certain key concepts: intelligence governance including control, authorisation and oversight; second, the difficulties facing oversight, specifically, how these can be alleviated by a structure involving both parliamentary and expert bodies and, third, the challenges presented by the structures of surveillance corporatism and its reliance on bulk collection.

CONTACT Peter Gill pgill806@gmail.com

© 2020 Informa UK Limited, trading as Taylor & Francis Group

Unfortunately, space permits no discussion of other important oversight actors such as civil society organisations and media.

Analysing intelligence governance

It is now a commonplace to assert that the intelligence problem facing western and many other states has changed significantly since the end of the Cold War. The 'puzzles' of the Cold War have been replaced not just by greater 'mysteries' but also by the complexities of the globalised world.[1] Thus, 'The essence of intelligence is hardly any longer the collection, analysis, and dissemination of secret information, but rather the management of uncertainty in areas critical for security goals for societies'.[2] Intelligence has always worked predominantly within the 'uncertainty' segment of the risk and probability continuum but now we are even uncertain about the presence or location of a threat and the harm it could cause as well as the efficacy of our methods for assessing it.[3]

Democracy requires that governance must be established in law – historically this was a very uneven process – but now governing statutes are the norm, at least in democratic and many hybrid[4] regimes, for establishing both the agencies and the oversight process. Compared with thirty years ago, the law is now playing a much more significant role in intelligence governance, for example, the role of the European Court of Human Rights (ECtHR) in setting out the required principles since the 1970s. But while law is a necessary condition for democratic governance it is not sufficient: law both empowers and limits agencies and there is a danger of 'legalism', that is, that legal forms/processes present an appearance of propriety behind which unreconstructed practices continue. For example, law plays a much greater role now in operations. Lester describes the process of planning covert action in the CIA and how lawyers are embedded at each level of internal authorisation,[5] and quotes an intelligence officer: 'in private practice, the attorney's objective is to limit risk by making sure the client stays well within the law. In bounding intelligence, the attorney provides the service of finding how close to the law the client may come before breaking it'.[6]

Vague and general wording in intelligence laws may reinforce the normal degree of ambiguity inherent in statutes[7] which, in turn, enables the continuation of 'plausible deniability' for ministers and even for overseers. For example, the UK ISC either did not understand or professed ignorance of the extent and complexity of mass surveillance exposed by the NSA/GCHQ files leaked by Snowden[8] and which had developed under the Regulation of Investigatory Powers Act (RIPA) 2000. Subsequently, the then UK Interception of Communications Commissioner (a former judge of the Court of Appeal) described RIPA as 'an extremely difficult Act of Parliament to get your mind around'[9] and David Anderson, a senior barrister and the UK government's counter-terrorism reviewer, described it as 'obscure since its inception … patched up so many times as to make it incomprehensible to all but a tiny band of initiates'.[10]

As democrats, what is our objective? Through democratic debate and law, to secure governance of intelligence adequate to establish public confidence regarding its efficiency, effectiveness and propriety. Efficiency refers to sound budgeting and expenditure control, effectiveness refers to the success or otherwise of intelligence production and propriety includes not just the legality of what agencies do but also that it is ethical. Thus, governance is integral to the organisation and processes of intelligence and has three 'stages': control, prior authorisation and oversight. The relationship between them is summarised in Figure 1:

Control

The criteria for internal management and direction of intelligence are the first condition of 'democratic' governance, including:

- professional heads of agencies,

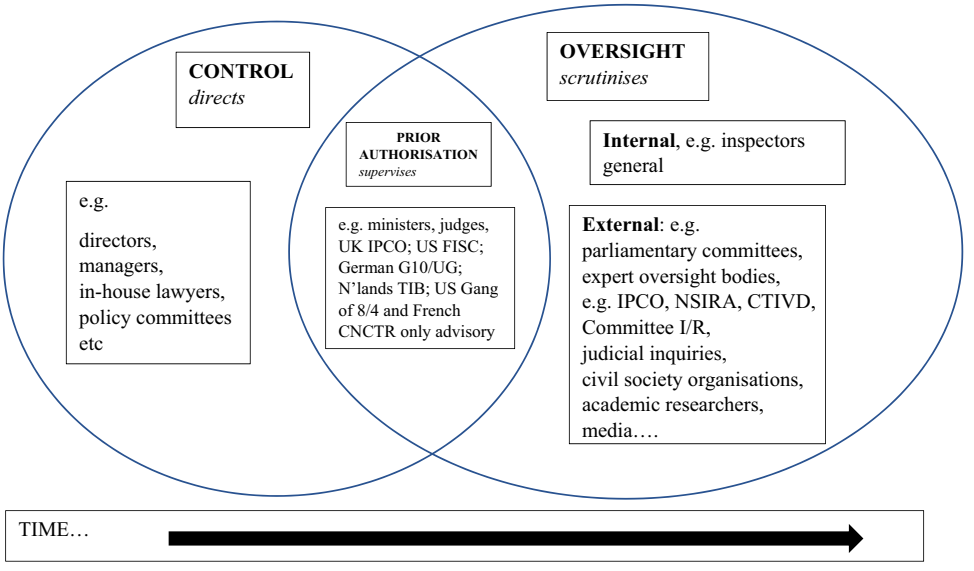

Figure 1. Intelligence governance.

- policy determined by elected ministers,
- staff recruited on merit,
- training in tradecraft and human rights,
- rules for intelligence-sharing,
- mechanism for internal review of legality.

The literature on this subject is scant; insiders have little interest in talking about it and outside researchers cannot access the processes involved. We know more about recruitment and training than we did[11] but this article concentrates on authorisation and oversight.

Prior authorisation

Initial decisions as to what information collection and operations an agency wants to conduct will be determined internally; normally the more intrusive the operation the higher-up should be the decision-maker. But a key feature of democratic governance is that, before the operations are conducted, they should also be authorised by someone outside the agency. This might be a minister, but greater independence exists if it is a judge, perhaps sitting in a specialist court such as the US Foreign Intelligence Surveillance Court (FISC). This was originally created because of the evidence revealed by the Church Committee hearings into the extensive domestic intelligence gathering conducted during the Cold War.[12] The Foreign Intelligence Surveillance Act (FISA) limited a President's authority to gather foreign intelligence and established the procedures by which agencies must satisfy the court in order to obtain an authorisation. Only a very low proportion of applications to the court were ever rejected entirely[13]; yet the Bush administration still saw fit to avoid the procedures after 9/11 in its Terrorist Surveillance Programme (wound up in 2008). Overall, the court has never escaped from the information asymmetry which bedevils all external institutions of authorisation and oversight.[14] This has most recently been demonstrated by the report of the Justice Department's Inspector General into the FBI's Russia investigation during the 2016 election campaign which 'uncovered a staggeringly dysfunctional and error-ridden process in how the FBI went about obtaining and renewing court permission under FISA, to wiretap Carter Page, a former Trump campaign adviser'.[15]

The German 2016 post-Snowden law creates an Independent Committee (UG) for the prior authorisation of 'strategic' communication surveillance (i.e., bulk collection). It will be located at the federal court of justice in Karlsruhe and consist of three members – two judges and one prosecutor – appointed by the government, to meet at least every three months and with the power to invalidate measures it finds unlawful or unnecessary. Essentially, this complements the pre-existing G10 which only has jurisdiction where surveillance will involve German citizens or people in Germany whereas UG will deal with foreign-foreign surveillance. In the Netherlands, a Review Board for the Use of Powers (TIB) assesses in advance whether an authorisation for the use of 'special' investigatory powers by the military or civilian agency granted by the Minister is lawful.[16] Similarly, in the UK once a minister has signed a warrant authorising the agencies to use cover measures, it must be authorised also by the Investigatory Powers Commissioners Office (IPCO) under what is called the 'double lock'.[17] Sometimes the national body can only advise on, not determine, the use of covert powers, for example, in France since 2015 the *Commission nationale de contrôle des techniques de renseignement* (CNCTR) has acted as advisory administrative body to ministers on whether intrusive surveillance measures should be applied.[18]

Oversight

If control 'directs' intelligence operations and prior authorisation 'supervises' them, then oversight carries out 'scrutiny' in the pursuit of efficiency, effectiveness and propriety. Depending on the specific legal and institutional rules, scrutiny may take place before, during and after the fact but, in general, increases as time passes from the actual conduct of the operation.[19] Oversight must be distinguished from 'accountability' which requires officials to explain actions and to suffer the consequences or put the matter right if errors are made.[20] Oversight is a precondition for accountability. If there is no scrutiny of an official's performance, then they cannot be held accountable (unless they are extremely honest in coming forward with their own confession.) Oversight must be of all aspects of organisation, information gathering, analysis, dissemination and operations within the intelligence 'web' but is not for micromanagement: there is a danger if, for example, parliamentarians seek to determine targets because it politicises, in a bad way, agency operations leading potentially to inefficiency and corruption.

The first level at which oversight must take place is *within* the agencies. Inspectors general (IGs) are the most common institution; in the US they are appointed by the President subject to Senate confirmation, with the mandate to fight fraud, waste and abuse by means of audits and investigations and they report both to agency heads and Congress. Given the strength of organisational cultures, this 'boundary-spanning' role has proved highly uncomfortable for its occupants because of its place within, say, the CIA, yet with obligations to report to Congress.[21] There are around a dozen inspectors general in the US intelligence community and current controversy exists because several have been accused of failing to protect whistleblowers – one of the primary functions for IGs when their mandate is the investigation of fraud, abuse, waste and misconduct.[22] But in April 2020 the IG for the Intelligence Community, Michael Atkinson, was sacked by Donald Trump, for having not only protected a whistleblower but reporting as 'credible' their complaint about Trump's interactions with Ukraine to Congress.[23] Australia, South Africa and Bosnia–Herzegovina are examples of other countries where IGs have the primary function of strengthening executive oversight though some also report to parliament.

External oversight of intelligence will take place both within the government and outside. Except where security agencies are literally 'rules unto themselves', their parent governments will exercise some degree of oversight, though this may well include ministers preferring to 'plausibly deny' agency actions. As well as 'boundary-spanning' links between the internal and external overseers,[24] external bodies scrutinising the same agencies should also be linked. Oversight systems that have developed piecemeal over time have been especially prone to failure in this respect. In Canada, for example, Justice O'Connor reviewed Canadian and foreign oversight

experience while conducting his inquiry into the US rendition of Maher Arar to Syria in 2002 and proposed a structure that would have the separate agency review bodies (SIRC, CSE Commissioner, RCMP Complaints Commission) co-operating in cases where the agencies themselves co-operated operationally and shared information.[25] No action was taken on this report in 2006 but it seems to have inspired some of the changes made a decade later and which are discussed below.

What is required for effective oversight?

The central requirements are well understood and can be summarised as:

- Clear statutory mandate;
- Independence from the executive, including separate, secure location;
- Appropriate investigative powers including right to access information;
- Quality membership and adequate resources to employ expert staff;
- Ability to maintain secrecy and thus gain trust of agencies and public; and
- Political will to use powers in fulfilling mandate.[26]

What are the difficulties facing oversight?

Mandate and trilemma

Most oversight bodies have a mandate for just one of effectiveness, cost (efficiency) or legality/proportionality or, if the mandate includes two or three, will normally focus only on one or two 'because of the impossible task of successfully addressing all three elements … an impossible trilemma'.[27] Dietrich shows how the trilemma potentially exists in Germany:

> The *lawfulness* of intelligence activities is, however, not the only criterion of intelligence oversight. … the parliament does not only oversee lawfulness, but also the *usefulness* of intelligence activities. … Also, *efficiency* and *effectiveness* of intelligence services are criteria which can be derived from the German constitution.[28]

However, the three roles were carried out by separate bodies: first, the *Parlamentarisches Kontrollgremium* (PKGr) which started on an informal basis in 1956, and was put on a legal footing in 1978.[29] The *Vertrauensgremium* (the Trust Committee) is responsible for budget control and the G10 Commission (not necessarily members of Parliament) is responsible for finally authorising surveillance operations once they have been approved by the relevant minister. These three hardly interacted with each other before the 2016 reform; in fact, secrecy requirements prevented any systematic exchange between them.[30]

Resources and will

With one possible exception – the well-endowed US congressional committees,[31] parliamentary oversight committees lack adequate resources of time and expertise. Elected politicians are busy people with a variety of demands on their time, possibly from other committees as well as general work in relation to legislation and concerns of their voters. As an area of interest, intelligence is arguably more complex than, say, transport, education or housing, and it will take some time for members to work out what questions they should be asking, never mind evaluating the answers they get. It is hard work and there may not be much for elected politicians to show for their efforts, which might also explain any lack of political will to exercise their mandate. In former authoritarian states, parliamentarians may have understandable reluctance for some time to tangle with security and intelligence agencies. Even in the US, Zegart & Quinn's comparison of committee hearing activities, legislative productivity and interest groups across different policy domains between 1985 and 2005

showed that intelligence almost always ranks at the bottom, in part at least because of the weak electoral pay-off in intelligence.[32]

When the ISC first investigated the July 2005 (7/7) London bombings, they 'just listened'[33] to what they were told by senior agency officials, having neither the will nor resources to do anything else. Only when the shortcomings of their May 2006 report[34] emerged in 2007 and the ISC returned to the case, did they carry out a more thorough investigation: 'We have gone even further into the detail, looking at the raw evidence – reviewing operational documents, surveillance photographs, transcripts of conversations, police action logs and covert recordings'.[35] Certainly, the 2009 report reflected increasing understanding among the members and provided much operational detail of interest to students of counterterrorist intelligence, as does the subsequent material produced by the inquest into the deaths that occurred on 7/7.[36] As a result of the 2013 reforms, ISC has been able to employ more staff and by 2017, had seven 'core' staff including greater technical expertise and another seven worked on the inquiry into the allegations of collusion by UK agencies in rendition and torture.[37]

From secrecy to asymmetric information

Compared with other policy areas, there are specific problems in governing intelligence which, with its special surveillance powers, has developed in modern states as a largely self-referential system within a 'ring of secrecy'. Security agencies cultivate this even with respect to other government departments.[38] The relationship between secrecy and transparency during the Cold War in western powers was essentially zero-sum, and this is still true of authoritarian states.[39] Security knowledge is now spread so much more widely through democratic governments, the private sector and even civil society in the context of counter-terrorism that some argue that the 'protective state' has replaced the 'secret state'.[40] This should not be overstated; however, since there is still a major difference between what states seek to know about citizens and what citizens are permitted to know about states' security operations.[41]

While secrecy is necessary to safeguard aspects of agencies' work, specifically their sources and methods, it may also be used to protect agencies/government from embarrassment or being held accountable for wrongful actions. Colaresi also argues that the 'secrecy dilemma' is not a simple zero-sum trade-off between secrecy and transparency but, from a normative perspective, because the relationship is modified by the role that time plays in allowing for subsequent oversight [cf. the 'time' arrow in Figure]. Therefore, effective institutions of oversight and higher transparency can increase the security of countries through increasing the public's trust in governments compared with the lower levels typical of illiberal regimes.[42]

But, if the contest is no longer zero-sum, it is still very uneven: 'The core of intelligence and accountability is the problem of asymmetric information. Information is key to the process of intelligence programs, and thus it is highly guarded within the executive branch.[43] Yet, taking a different tack, Aldrich & Richterova argue that the nature of privacy has, in fact, changed relatively slowly over the last decade and instead that these developments (Snowden, Manning leaks, etc.) denote a 'crisis of secrecy'. The key issue is not government looking at us, but our increasing ability to look at government, and especially new ways of calling the secret state to account.[44] Yet the consequence has not been any radical reduction of state surveillance capacities but, rather, having them freshly legalised along with limited reforms to authorisation and oversight (see discussion of German and UK 2016 legislation below).

Self-referential secrecy systems within intelligence agencies also enhance the power of organisational culture. It is a well-established feature of organisational life that 'working cultures' adopted by staff will often diverge somewhat from the official published regulations and decision hierarchies. These cultures can be even more impervious to outside influence when the employees share a mission such as upholding law or protecting national security. Different organisational roles produce different sub-cultures, for example, Lester refers to several cultures within the CIA.[45]

These can hamstring external oversight: while breaking the internal rules of the CIA will be swiftly punished, the 'breaking of external constraints' is considered an acceptable form of executive behaviour.[46] Similarly, when it comes to international cooperation, agencies will be more highly regarded by their foreign peers to the extent that they can preserve information from the gaze of overseers.[47]

Therefore, even where legislation formally enables untrammelled access for overseers, committees will still need to deploy skill in negotiating with informal gatekeepers in ministries and agencies and there are likely to be disputes. Jennifer Kibbe, for example, describes the problems faced by US intelligence committees because reports they request are not provided, briefings are vague and staff may not be permitted to attend.[48] The judicial commissioners in the UK have also faced this problem; the UK Intelligence Service Commissioner's 2015 annual report regarding their dealings with Adebelajo, one of the killers of Lee Rigby, was highly critical of SIS's reaction to his investigation:

> … SIS demonstrated a troubling tendency to be defensive and unhelpful, it provided inaccurate and incomplete information and generally sought to 'fence' with and 'close down' lines of enquiry, rather than engage constructively.[49]

Oversight: a 'ritual dance'?

Rittberger & Goetz note that new pressures towards accountability and transparency may provoke resistance from organisations who undertake symbolic reforms to comply with external demands' with the result that oversight amounts to an 'organised hypocrisy'.[50] Enabling law and organisational structures may be changed but the occupational culture may be untouched without reform of recruitment and training, increasing the potential for agencies to remain 'authoritarian enclaves'[51] or become 'deep states' immune to electoral changes in government.

Otamendi & Estevez develop a matrix of democratisation and governance with particular reference to Latin America and reach the conclusion that intelligence is in many cases still an authoritarian enclave operating '… with an opaque logic, conducting political intelligence for the ruling party or by selling their services to the highest bidder. In addition, its opacity, lack of real control, but high budgets and access to sensitive information, places them in a position of power in the shadows with ability to influence and blackmail political, judicial and economic actors, among others'.[52]

In Central and Eastern Europe '… state experiences indicate that the prospect of gaining NATO membership may have spurred certain reforms in intelligence governance, but that these were not aimed at increasing the democratic control or accountability or good governance of the intelligence sector'.[53] Aldrich & Richterova also show that official accountability mechanisms imported from the West have proved ineffective.[54] Romania provides a well-documented case: Many of the post-1989 reforms have been only superficially implemented and monitored, particularly after Romania joined NATO and the EU. Consequently, there has been '… in the last 15 years a trend towards the "secretization" of oversight within the parliament, as concerns for secrecy prevailed over the responsibility to inform the public about intelligence accountability'.[55] Zulean and Şercan agree and suggest further that the attempt to create a new 'security culture' in Romania via the creation of military, police and intelligence academies has resulted in positive public awareness activities but also, through the award of diplomas and degrees, in the creation of a new elite which could amount to a nascent deep state resisting democratic control.[56]

But the older democracies have not been immune from largely symbolic reform: Lester's core argument is that the interrelationships of external and internal accountability in the US have led to it being easier for agencies to keep secrets.[57] In France, the 2007–2008 reforms reinforced the effectiveness of the French intelligence organisation rather than created a specific legal framework. Hence, the form of parliamentary control established in 2007 was embryonic with parliament having only very limited powers and the vague mission of 'monitoring' the intelligence services.[58]

Most parliamentary committees will be controlled by the majority – or governing – party and therefore may simply be unwilling to criticise the agencies formally controlled by senior members of their party. For example, Laurie Nathan says this remains a problem in South Africa where ruling party members of the committee 'work under instructions and don't make a fuss about intelligence publicly'.[59] Similarly, in Serbia where committee members 'are under strong political control'.[60] Again, the problem is not limited to new democracies; Kibbe shows that partisanship has been a major factor hampering the performance of US intelligence committees since 1990.[61]

Energetic and informed oversight will create tensions with the agencies; if there are no tensions, then the oversight system is simply not working. Handling them is crucial: if they become too serious and agencies will not cooperate at all with overseers then the system will be broken. Lester argues that the tensions between executive and legislature in the US, which she describes as 'oppositional oversight', have driven changes so that there is 'collaboration' which incorporates both sides.[62] Hijzen discusses the development of parliamentary oversight in the Netherlands where the Committee on the Intelligence and Security Services (ISS Committee) consists just of heads of the parties represented in Parliament and had little impact, being passive and reactive, just listening to explanations from officials in a 'ritual dance' where little serious criticism was heard.[63]

Both parliamentary and specialist investigative bodies are required

Clearly, parliaments have the required status and legitimacy for the oversight task but often lack the necessary time, expertise or political will to act vigorously. The advantages of specialist bodies include greater expertise and time and less risk of political division. Like parliamentary committees, their mandate may vary between efficacy, legality, etc., and they may also have authorisation functions regarding covert measures (such as IPCO). Their legitimacy can be increased by giving parliament a role in appointing them and receiving their reports. On the other hand, if they operate effectively, they can gain public legitimacy by delivering where parliament fails, for example, the Ombudsman and Commissioner for Information of Public Interest in Serbia.[64] Wegge notes that his expert interviewees generally saw parliamentary committees as less reliable than appointed expert bodies in keeping secrets and not using classified information for political gain.[65]

In Belgium Standing Committee I (Intelligence; or R – *renseignement*) has three members appointed by the Senate and has both administrative and investigative staff. The committee reviews the legitimacy and effectiveness of and coordination between the (civilian) State Security, (military) General Intelligence and Security Service and Coordination Unit for Threat Assessments (a fusion centre). It can undertake investigations on its own initiative, at the request of the Senate or in response to a complaint from a citizen or whistleblower. In the Senate, there is a five-person monitoring commission that meets regularly with Committee I to discuss its work.[66] Since 2002 the Dutch CTIVD has provided more detailed and thorough oversight of the legality of the agencies but the parliamentary committee still labours under the 'structural and cultural constraints inherent in Dutch oversight practice'.[67] In essence, in both Belgium and Netherlands, parliament delegates the detailed investigative work of oversight to these specialist committees while retaining their general prerogative to challenge the executive.

A similar trend towards oversight combining both parliamentary and specialist bodies can be seen now in Canada, Germany and the UK. Farson & Whitaker argued that the Canadian government view of oversight was essentially negative; it was seen as a grudging response to specific problems in individual agencies, rather than as a potentially useful tool for improving the effectiveness of the network of agencies.[68] The Canadian Security Intelligence Service Act 1984 created the civilian CSIS after the McDonald Commission had exposed the illegal activities of the RCMP Security Service.[69] Shrinking from the prospect of parliamentary oversight at the time, the Government set up the Security Intelligence Review Committee (SIRC), an external specialist body, but, despite its title, with a mandate only over CSIS. Similarly, in 1996, the Government responded to (or took advantage of) publicity concerning Canada's SIGINT agency, the Communications Security Establishment (CSE), by

appointing a commissioner with similar powers to SIRC to review CSE activities to ensure compliance with law, respond to public complaints and report at least annually to the Minister of National Defence who tables it in Parliament. After off and on deliberation for many years, in 2017 Canada finally joined the mainstream of democracies by establishing a 'committee of parliamentarians', clearly modelled on the original UK ISC, and which may have up to 11 members, eight from the Commons, and three from the Senate.[70] Its first annual report was published in April 2019 and provided a review of Canada's defence intelligence activities and how the country sets intelligence priorities.[71]

Almost simultaneously the extra-parliamentary governance structure was also amended; an Intelligence Commissioner (similar to UK IPCO) was created to review and approve (or not) ministers' authorisations of various covert activities by CSIS and CSE. On oversight, the change built on that recommended by Justice O'Connor to overcome the compartmentalisation of oversight: the SIRC, Office of the CSE Commissioner and the RCMP Civilian Review and Complaints Commission would be merged into a new National Security and Intelligence Review Agency (NSIRA) to oversee the legality, reasonableness and necessity of the agencies. Its reports to ministers would be classified but it will also produce an annual unclassified report to Parliament summarising the recommendations made to ministers.[72]

The Snowden files provoked an outpouring of media scorn for the German system: the *Frankfurter Allgemeine Zeitung* (FAZ) described 'Powerful Agencies, Toothless Windbags'; an article in the liberal newspaper *Die Tageszeitung* described a meeting of the PKGr as 'In the Assembly of the Clueless', and the German news magazine *DER SPIEGEL* wrote about 'German Intelligence Services Out of Control'.[73] There are three main reforms as a result of the 2016 BND law. As we noted above, an Independent Committee (UG) has been established for the prior authorisation of 'strategic' communication surveillance (bulk collection). There was no reform of the G10 itself, which remains seriously under-resourced for a body intended to carry out serious oversight. Second, a permanent intelligence oversight coordinator will attend the meetings of each of the PKGr, G10 and Trust Committee, carry out investigations on behalf of the PKGr (and may also be tasked by the Trust committee). Third, more than a dozen full-time staff will be appointed to a secretariat to support the PKGr. Changes to control/coordination include a new position of Secretary of State for Intelligence Services Issues.[74]

In the UK, the Snowden revelations were followed by three inquiries, one by the ISC, one by the Royal United Services Institute (RUSI) set up at the behest of the then deputy PM and a third by David Anderson QC, the counterterrorism reviewer. On the issue of prior authorisation, both RUSI and Anderson argued that judges should be involved in the authorisation of all covert surveillance, and this is the model for the IPCO in the 2016 Act.[75] IPCO's role is to keep under review the majority of the targeted and bulk surveillance powers available to the intelligence services, especially with regard to privacy protections. The agencies are required to disclose all the necessary information the Commissioner requires and to assist her in accessing apparatus, systems or other facilities of the intelligence services when exercising oversight functions. She must report at least annually to the PM and the office is assisted by a new technical advisory panel. IPCO is not just a responsive institution and may conduct thematic reviews of capabilities and investigate serious errors on its own initiative. The 'compartmentalisation' of oversight has been addressed to some extent: the Act contains a power for the ISC to refer matters to the IPCO for investigation, inspection or audit. In such cases, IPCO retains discretion over whether to investigate but, importantly, where an investigation is held, the Prime Minister is obliged to share the report with the ISC.[76]

It is early days for this new structure but it certainly reflects progress in providing the potential for more energetic and joined-up oversight, for example, IPCO was in daily contact with MI5 over the mishandling of material from intercepts, specifically, that material was more widely shared than it should have been. This was reported to IPCO by MI5, not revealed through external oversight, and perhaps this reflected greater trust and/or wariness of IPCO inspectors than would have been the case with ISC.[77] But, arguably, it suffers from the basic error of combining the authorisation of covert

surveillance with the oversight thereof, such that conflicts of interest are bound to arise within the single office, a view endorsed in the RUSI report.[78]

Considering European and Canadian experience, the Snowden disclosures have had little impact on the ability of intelligence agencies to carry out surveillance of the Internet but have seen some of the most far-reaching reforms for decades in control, authorisation and institutional changes to oversight – it remains to be seen whether the new structures and the political will of those acting as overseers will actually deliver.[79]

New twenty-first century challenges

At the outset, the challenge presented by the radically changed nature of intelligence 'problems' in the twenty-first century was outlined. Here, we consider two further, and coincident, developments that must be addressed. First, the revolution in information and communication technologies which now not only generate data in unprecedented quantities but also provide increasingly sophisticated means for its processing and analysis and, second, a mushrooming of networks of cooperation between intelligence organisations. Both developments pose urgent governance challenges.

The relative certainties of the Cold War – who was the enemy, where they were, what they could do – have been replaced by much greater uncertainties – who are they, where are they, what can they do? Yet intelligence has sought to contain the new uncertainty within old frameworks of risk and by collecting ever-more data.[80] It is not always clear that this information can be translated into 'knowledge', but bulk collection is certainly the basis for new forms of power. Most significantly, the major corporations turn this raw material into the means of behavioural modification[81] which is at the core of the surveillance capitalists (google, facebook et al. …) project to unify information and control in what Zuboff calls instrumentarian power.[82] Since intelligence is future-oriented with a goal to prevent bad things happening, it is caught up in the same dynamic: 'Governments now turn to instrumentarian power as the solution to (terrorism as a) new source of societal uncertainty, demanding the certainty machines that promise direct, reliable means of detection, prediction, and even the automatic actuation of countermeasures'.[83] Drones would be the clearest contemporary example of an automatic measure but there are others, for example, facial recognition triggering arrest or exclusion from buildings.

A much wider variety of institutions in democracies are involved in intelligence and its governance than, say, thirty years ago and the literature of Intelligence Studies has increasingly acknowledged this,[84] but most analysis still concerns cooperation (or its absence) between state agencies. Non-democratic regimes have always sought to enlist a wider range of people and social organisations into the net of surveillance, but everywhere now a variety of corporate partners, social institutions and individual citizens have become central participants in the collection of intelligence information'.[85]

There is a broader context here that might be characterised as a 'new medievalism': the decentering of states (upward to international institutions and downward to localities) and the increasing significance of private corporations in security and intelligence. There is almost complete material interdependence between security corporations and modern states as the state relies on the corporate sector for infrastructure, advice, software and hardware while, in return, corporations are dependent on states for contracts and the legal framework within which they work.[86] Institutionally, this material interdependence and ideological consensus mean that states govern security through private corporations and also civil society organisations, sometimes even para-states, that are effectively immune from democratic governance.

Given the coincidence of state and corporate goals, it is not surprising that an almost symbiotic relationship has developed between the agencies and the communication service providers (CSPs). From the perspective of IS, therefore, what we are dealing with is not just the 'surveillance capitalism' dissected by Shoshana Zuboff (2019) but also a security or surveillance corporatism. As I have argued elsewhere, there are three main characteristics of the new security corporatism; secrecy, an almost

complete material interdependence between security/communication corporations and modern states, and, third, a resulting ideological consensus covering the self-regarding profit-seeking corporations and governments' national security policies.[87] This 'interdependence' does not mean there are no disagreements between the parties; there is a clash between the corporate claim to protect customers' privacy and the agencies' collection of data on the same people, as witnessed by the CSPs anger when Snowden's files revealed the extent to which their systems had been hacked by the agencies.

Zuboff discusses the specific relationship between Google and the intelligence agencies: before 9/11 legal moves were afoot in the US to regulate online privacy but the attacks

> … transformed the government's interest in Google, as practices that just hours earlier were careening toward legislative action were quickly recast as mission-critical necessities. Both institutions craved certainty and were determined to fulfil that craving in their respective domains at any price.[88]

Even though Poindexter's Total Information Awareness program did not obtain congressional support, Google developed data-mining initiatives for the NSA and IC 'Intelink' intranet which was funded otherwise. Google benefited both from direct sponsorship and informal networks and from the fact that it operated within a space relatively free of the legal constraints surrounding US government agencies.

However, there is one significant respect in which the object of intelligence differs from that of the profit-maximising CSPs. Zuboff notes the 'radical indifference' of the companies to the content of communications: they do not care what we think or do as long as they can count the clicks.[89] This explains the great difficulty governments have in convincing companies to remove harmful material from social media and the internet, but intelligence agencies do care what we think and do. The only way in which they can possibly achieve their preventive goals is by distinguishing communications that indicate harmful intentions and capabilities from those that do not. Thus, seeking the means of behavioural modification remains a dream for securocrats everywhere, as does the possibility of 'replacing society with certainty' and finding the answers to questions that have not even been asked.[90]

What are the prospects for the oversight and regulation of this new security corporatism? ECtHR has already made some key decisions regarding mass surveillance, for example, *Big Brother Watch and Others v. the UK* (no.58170/13) that did not outlaw mass surveillance *per se* but requires strict requirements for authorisation and oversight but, most recently the Grand Chamber of ECtHR decided to consider a definitive judgment on the compatibility or otherwise of mass communication surveillance with the ECHR and the hearing was scheduled for July 2019.[91]

Wetzling & Vieth provide a compendium of good intelligence governance practices in Australasian, European and North American democracies with respect to bulk foreign communication surveillance. These include that authorisation bodies should have sufficient expertise and independence, that oversight committees be informed of international cooperation agreements, that the standards or proportionality assessments be discussed with civil society bodies, that overseers may be given direct access to agency data systems, that data processing be subject to regular review and random checks, that oversight ensures some human element exists within analytical systems, and that national oversight bodies seek to cooperate in order to enhance their effectiveness as in the European example discussed below.[92]

Such efforts are underway: van Laethem reports that CTIVD draws on a pool of security-cleared experts from different backgrounds.[93] But the Dutch review body is already looking a step further: it explores the use of computerized data processing in oversight itself, for example, by automatically comparing the data processed by the services, with the aim of being able to recognize any processed data deviating from the standard. In other words, the CTIVD looks at data-driven forms of oversight that it may apply prior or in addition to its thematic lawfulness investigations. This will enable it to gain a broader understanding of any risks of unlawful data processing by the services'.[94] Such measures may reduce the informality of intelligence sharing that plagues both managers and overseers, but they cannot eliminate such working practices entirely. Just as Thorsten Wetzling &

Kilian Vieth point to the importance of a human element being retained at key points of an intelligence process dominated by automaticity, so it is with oversight: overseers will still need to spend time talking with officials in order to gain insight into decision-making.[95]

Vieth and Wetzling have developed the work required so that oversight laws are complemented by practical measures. Their proposals include direct access for oversight bodies so that the filters used for data minimisation are appropriate, that pattern analysis can be applied to log files to check for anomalies, that there is digital documentation of warrant authorisations and that there should be systematic exchanges between oversight bodies and the corporations involved in collection.[96] This last point acknowledges the new corporatist reality: bulk collection is footloose and can be conducted remotely; thus, whatever privacy protections are provided by the state for its citizens, the corporate collectors maximise what they can take as core of their business model.[97] A crucial aspect of control and oversight, therefore, is what practical and legal restrictions there are on state agencies accessing the vast data warehouses.

This architecture does not just incorporate public and private sectors, it has also expanded spatially. Transnational intelligence cooperation is not new, for example, between allies during wartime, and the UKUSA established a global SIGINT network immediately after WWII. NATO and Warsaw Pact 'networks' were extensive during the Cold War but the post-Cold War world has seen a proliferation of multi-dimensional networks. Lefebvre identified a number of factors that will influence the nature and extent of international cooperation: different perceptions of threat and the foreign policy objectives of the respective states, asymmetrical power relations between states, their view of the human rights records of a potential partner, differences in legal parameters and standards, and the fear of disclosure of information given any previous experience of shared intelligence being misused.[98]

Whether cooperation takes place formally or informally, the main rule for information sharing is Originator Control (ORCON), that is, information may not be passed to a third party without the permission of the originating agency. This has presented a stumbling block to most attempts at overseeing international cooperation; agencies have rarely, if ever, granted permission for their information to be shared with another country's oversight body. Yet there are arguments for and current examples of attempts to establish transnational oversight arrangements. As a first stage, CTIVD argues that 'Not only should the choice to cooperate with a foreign service be thoroughly weighed beforehand, but the actual cooperation in practice – for example, providing personal data, executing joint operations or providing support to a foreign service – must also be provided with sufficient safeguards. With respect to these two themes, the ISS Act 2017 offers an enhanced framework that aims to protect citizens' fundamental rights. One example is the requirement that the collected data should be assessed for relevance as quickly as possible and immediately destroyed when not relevant. Another is that unassessed data may only be issued to a foreign service after authorization of the Minister and that the CTIVD must be notified'.[99] This was precisely the problem in Canada just after 9/11 when the RCMP provided the FBI with unassessed, and highly misleading, information about Maher Arar that led to him being rendered to Syria where he underwent torture.[100]

Some initiatives can be carried out by national oversight bodies acting alone; the next stage is harder: 'For intelligence to be seen as a public good, oversight responsibility must be shared amongst all nations involved in multilateral agreements to avoid asymmetry in relationships.[101] For example, Aldrich argues that, if states can agree on complex information-sharing agreements, then, surely, they can agree on an oversight process such as a former head of national service, acting as a roving Inspector General.[102] Where there is a multinational governance framework in place, it might be easier to develop such arrangements. In the EU, for example, 'While information sharing among secret services in the EU is still mostly informal and unregulated, police intelligence sharing inside the EU has become more institutionalised and bound to a regulatory framework'.[103] De Ridder reports that European intelligence services did agree to set up a permanent platform and common database in the wake of the 2015 Paris attacks.[104] CTIVD has recommended a joint framework for cooperation between the 30 countries involved in the Counterterrorism Group (CTG) that would

apply to all participating countries and be based on data protection principles, for example, in which cases personal data could be stored in databases, the reliability of that data, keeping it up to date, management of the database.[105]

There is an obvious clash between overseers' national authority and transnational intelligence networks. Yet, there have been efforts by overseers to meet periodically for some years, for example, most recently the UN's International Oversight Forum met in London in October 2019.[106] But more systematic attempts to grapple with the complexities of transnational oversight are being made: oversight bodies in Belgium, Denmark, Norway, Switzerland and Netherlands have collaborated since 2015 regarding international intelligence cooperation:

> … A valuable and necessary step towards closer oversight cooperation is to minimize secrecy between oversight bodies. Once data has been exchanged by intelligence services, there is no need for oversight to lag behind …..[107]

The UK IPCO has now joined the group and is also part of the Five Eyes Intelligence Oversight and Review Council.[108] But these efforts represent just a few faltering steps on a long, hard road: different national overseers have different powers and mandates, they may worry about the reaction of their own agencies if they collaborate, the topics covered are very sensitive and, consequently, building trust between bodies takes time.[109]

The universal problems for overseers and regulators are knowledge and power: they cannot know as much about agency's activities as those performing them and they have only limited capacity to change agency's behaviour even if they come to believe it is necessary. The combination of these two problems has led to the widespread disparagement of regulation, especially its 'command and control' version which is seen to lead to widespread inefficiencies. De-regulation has been central to neoliberal governance since the 1980s but has not resulted in its abolition; indeed, to the contrary, twenty-first-century governance, in which states seek both to befriend and control business,[110] has seen varieties of what can be called decentred regulation. Julia Black identifies the 'hallmarks' of these strategies as hybrid (state and non-state actors), multi-faceted (using different strategies simultaneously or sequentially) and indirect (involving coordinating and steering).[111] Similarly, Neil Quarmby draws on Malcolm Sparrow's work to show a spectrum of regulatory models: 'enforcement-based', 'engaged and responsive', 'self-regulation' and 'industry regulated'.[112] In theory, law can compel a state agency to cooperate with an oversight committee (even though in practice it may not ….) but law cannot command such cooperation from a private company. The relationship will be more one of negotiation and bargaining involving licensing, codes of practice, etc. The fragmentation of providers and their interdependencies, asymmetries of power between them and the sheer complexity of security situations means that oversight, like regulation in the private sector, will be at best decentred.

Research conducted into oversight of the corporate security sector identified three main types of failure: inefficiencies, human rights abuses and conflicts of interest. Perhaps unsurprisingly, the author found that the deficiencies in private sector accountability were not dissimilar from those well documented in the public sector: lack of political will, access to relevant information (complicated by the multiple layers of contractors and subcontractors), appropriate regulatory standards and the means to enforce change. Companies themselves may play a role as an 'accountability-holder', for example, by keeping government officials honest in their conduct of procurement processes, yet corporate self-regulation cannot be the whole answer and the rules must still be defined by government officials with their responsibility to protect the public interest. Either government officials or contractors may choose to act in their own organisational or personal interest at the expense of the public interest; thus, there is no alternative to encouraging greater commitment to oversee systematically the 'intelligence community', both public and private.[113]

Parliamentary and/or specialist oversight bodies must be empowered to extend their review over this corporatist intelligence architecture. For example, corporate codes of practice often suffer from

inadequate mechanisms for independent auditing; if these codes require the adoption of certain standards in order to be licensed, then companies could be required to 'buy-in' to public oversight mechanisms. Contracts for supply, training or other intelligence services from the state could only be made with companies thus signed up and the regulatory mechanism could be funded in the same way as the UK Financial Conduct Authority which levies fees on those companies who wish to operate in the financial sector.[114] A range of other issues would need to be determined, for example, would companies be under the same public reporting requirements as state agencies? If not, then, at a minimum, their license would depend on making their premises, personnel and files accessible to oversight bodies as part of monitoring their contract compliance or investigating complaints of human rights violations.

Conclusion

Discussions of intelligence oversight must examine the extent to which security intelligence can be maintained as a core democratic feature of liberal capitalist regimes. Yet, the task of overseeing intelligence in order to have any chance of holding agencies accountable is difficult and becoming harder. Van Laethem concludes that 'accountability gaps are growing as security agencies are receiving more legal powers and funds to work together, while review and oversight is still conducted in departmental and agency-based siloes'.[115] The gaps have widened further owing to the increased role of corporations as providers of hardware, software and data so that the emerging surveillance corporatism is arguably immune from oversight.

Yet there is a real conundrum here: while states are enmeshed in ever-more complex public-private networks, it is only they who can provide for 'democratic security' because they alone represent the public rather than a private interest.[116] Yes, the laws underlying state intelligence must be clarified and oversight arrangements strengthened but its capacities must also be enhanced in order to provide the basis for regulation of the corporate sector and repression of uncivil para-states. But because of limited resources and extensive transnational and cross-sectoral intelligence activity, state oversight is just one part of 'decentred regulation' which must also involve journalists, civil rights lawyers retained by non-governmental organisations (NGOs), regional bodies such as the Council of Europe and the European Parliament is required.[117] In other words, 'official' oversight must be complemented by *sousveillance*.[118]

Officials' suspicion of 'outsiders' can contribute to a confrontational environment if oversight concentrates solely on compliance. Therefore, overseers should beware excessive bureaucratisation and onerous reporting procedures and behaving such that agencies become risk-averse.[119] Similarly, Petersen & Tjalve criticise the idea that oversight via Weberian rules-based process is adequate for the new uncertainty and argue for greater emphasis on ethics-based judgment: 'What is involved in an ethos of judgment though, is a profound recognition of complexity and dilemma – an ethics of responsibility and a recognition of error, subjectivity and guilt which far exceeds legalist notions of simple 'right or wrongs'.[120] Therefore, oversight must beware over-legalisation; for example, quasi-judicial investigations looking for individuals to blame for failures should be replaced by political oversight which can benefit from the deployment of social science methodologies in order to examine organisational processes.[121]

But overseers must remain sceptical, avoid capture and maximise their access to people, places, papers and records. Regulation may be ineffective if, for example, it is based on predictable inspections and thus subject to 'gaming'. Experience with the democratisation of intelligence in post-authoritarian regimes shows that legislating for intelligence mandates and oversight is relatively straightforward but, while the new legal structures look very elegant, their impact is often more symbolic than real. To recall an earlier argument, overseers must resist becoming actors in a game of 'let's pretend …'; they must demonstrate energy, political will and develop expertise.

Clearly, the dangers for democracy have been aggravated by the development of corporatist surveillance structures. It is not hard to imagine what Eliane Glaser, 2018 describes as 'nationalistic

authoritarian capitalism'[122] developing given intelligence agencies' interest in security and order and their dependence on corporations for technologies and data. Agencies may easily become central elements of these regimes. Arguably this problem has just taken on a whole new and much-expanded reality with the widespread search by states and corporations for mobile data apps required for their 'track and trace' policies vis-a-vis COVID-19. Only the most vigorous control and oversight can enable us to escape from this danger in order to maximise the degree of democratic governance to which intelligence can be subjected.

Notes

1. Agrell & Treverton, *National Intelligence and Science*, 32-35
2. Ibid., 196
3. Gill, Intelligence, "Threat, Risk and the Challenge of Oversight," 213; see also Petersen & Tjalve, "Intelligence Expertise in the Age of Information Sharing"
4. 'Hybrid' regimes may be defined as those displaying elements both of democracy – somewhat competitive elections based on a degree of freedom of association – and authoritarianism – continuing restrictions on media, civil society and attacks on government opponents. Gill, *Intelligence Governance and Democratisation*, 50
5. Lester, *When Should State Secrets Stay Secret?*, 134-39. In the 1980s MI5 and MI6 shared one lawyer between them; it is safe to assume each has more now.
6. Lester, *When Should State Secrets Stay Secret?*, 73
7. cf. Edelman, *The Symbolic Uses of Politics*, 130-51
8. Cf. Leigh & Wegge, *Intelligence Oversight in the Twenty-First Century: Accountability in a Changing World*, ch.1.
9. ICC giving evidence to UK House of Commons Home Affairs Committee, 11 February 2014.
10. Anderson, "A Matter of Trust," 8.
11. For example, see ISC 2018
12. Church, *Final Report of the Select Committee to study Governmental Operations*.
13. Only 21 applications were completely rejected up to 2016 but in 2016 the number was 26 https://www.washingtontimes.com/news/2018/apr/26/fisa-court-denied-more-surveillance-warrants-2017-/
14. Lester, *When Should State Secrets Stay Secret?*, 159-204 provides detailed review of FISC
15. Savage, "We Just Got a Rare Look at National Security Surveillance."
16. CTIVD, *Annual Report for 2019*, 33
17. https://www.ipco.org.uk/
18. Warusfel in Leigh & Wegge, *Intelligence Oversight in the Twenty-First Century: Accountability in a Changing World*.
19. cf. Farson & Whitaker, "Accounting for the Future or the Past?," 678; Colaresi, *Democracy Declassified*, 234-39
20. cf. Aldrich & Richterova, "Ambient Accountability," 1006-07; Venice Comm, 2015, 4; Hastedt, "The Politics of Intelligence Accountability" and Lester 2015 focus specifically on the accountability question in the US
21. e.g., Lester, *When Should State Secrets Stay Secret?*, 56-70
22. McLaughlin, "Lawmakers Demand Investigation into Lack of Whistleblower Protections for Spies."
23. Savage 2020
24. CTIVD, *Annual Report for 2019*, 10; Gill, *Policing Politics*, 248-52
25. O'Connor, "Report of the Commission of Inquiry."
26. cf. Gill, *Policing Politics*, 248-53; Born & Johnson, *Who's Watching the Spies*, 235-38, Wills, *Guidebook*; Eskens et al., *Ten standards for oversight and transparency*.
27. Cayford et al., Plots, Murders, and Money," 1011-12, quotes at 1012
28. Dietrich, "Of Toothless Windbags, Blind Guardians and Blunt Swords," 400, emphasis added
29. Hillebrand, "Intelligence Oversight and Accountability," 307; Hegemann, "Toward 'Normal' Politics?" provides a case study of the PKGr since 9/11
30. Wetzling, "Intelligence Governance in Post-Cold War Germany," 177
31. Though, even here, the size and complexity of the US intelligence community, the complexities of congressional committee jurisdictions, members of the Senate and House committees' other commitments and limitations of secrecy mean that, arguably, they are just as under-resourced vis-à-vis the agencies as other overseers.
32. Zegart & Quinn, "Congressional Intelligence Oversight," 744
33. Michael Mates, speaking on *Newsnight*, BBC2, 19 May 2009.
34. ISC, *Report into the London Terrorist Attacks on 7 July 2005*.
35. ISC, 2009, para.11.
36. http://7julyinquests.independent.gov.uk/hearing_transcripts/index.htm,
37. ISC Press Release, 27 April 2017.
38. cf. Gill, *Policing Politics*, 79-82; Dobson, 2019, 11 and cf. Lester, *When Should State Secrets Stay Secret?*, 15-16

39. Gill, *Intelligence Governance and Democratisation*, 42-46 summarises the main differences between authoritarian and democratic intelligence regimes.
40. Hennessy, "From Secret State to Protective State"; Omand, *Securing the State*, 9-11.
41. Similarly, 'Surveillance capitalists know everything *about us*, whereas their operations are designed to be unknowable *to us*.' Zuboff, *The Age of Surveillance Capitalism*, 11, original emphasis.
42. Colaresi, *Democracy Declassified*, 234-39.
43. Lester, *When Should State Secrets Stay Secret?*, 205; see also Kibbe, "Congressional Oversight of Intelligence."
44. Aldrich & Richterova, "Ambient Accountability," 1003.
45. Lester, *When Should State Secrets Stay Secret?*, 41.
46. Lester, *When Should State Secrets Stay Secret?*, 21-2.
47. Wills & Born, *Who's Watching the Spies*, 286.
48. Kibbe, "Congressional Oversight of Intelligence," 33-38.
49. Intelligence Services Commissioner, "Supplementary to the Annual Report for 2015".
50. Rittberger & Goetz, "Secrecy in Europe," 839.
51. e.g., Otamendi & Estevez, "Intelligence Challenges in Latin America and Prospects for Reform."
52. Otamendi & Estevez, "Intelligence Challenges in Latin America and Prospects for Reform," 288.
53. Caparini, "Comparing the Democratisation of Intelligence Governance in East Central Europe and the Balkan," 522; see also Matei 2014.
54. Aldrich & Richterova, "Ambient Accountability," 1012-15.
55. Fuoir 2018, 57.
56. Zulean and Şercan, "Democratic Control of Romanian Intelligence after Three Decades," 15-16.
57. Lester, *When Should State Secrets Stay Secret?*, 6.
58. Warusfel, in Leigh & Wegge, *Intelligence Oversight in the Twenty-First Century: Accountability in a Changing Worl*, 127.
59. quoted in Pejic, 2018.
60. Petrovic, "Serbia," 328.
61. Kibbe, "Congressional Oversight of Intelligence," 38-42.
62. Lester, *When Should State Secrets Stay Secret?*, 106-07.
63. Hijzen, "More than a Ritual Dance," 235.
64. Petrovic, "Serbia," 329-30.
65. Wegge, "Intelligence Oversight and the Security of the State," 695.
66. van Lathem, 2011.
67. Hijzen, "More than a Ritual Dance," 237.
68. Farson & Whitaker, "Accounting for the Future or the Past?," 677
69. McDonald, 1981.
70. http://www.laws-lois.justice.gc.ca/eng/acts/N-16.6/page-1.html
71. (http://www.nsicop-cpsnr.ca/reports/rp-2019-04-09/intro-en.html)
72. (https://www.cse-cst.gc.ca/en/cse-act-loi-cst/accountability-responsabilite)
73. Dietrich, "Of Toothless Windbags, Blind Guardians and Blunt Swords," 397.
74. Dietrich, "Of Toothless Windbags, Blind Guardians and Blunt Swords," 401-02; Wetzling, *Upping the Ante on Bulk Surveillance*, 181.
75. RUSI, *A Democratic Licence to Operate*, 111-14; Anderson, "A Matter of Trust"; Investigatory Powers Act, 2016, Part 8, chapter 1 http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted
76. Foregoing based on Leigh, "Reappraising Intelligence Oversight in the UK," 86-88.
77. Bowcott, "Court Told MI5 Kept Material and Gained Warrants Illegally," 10. See also IPCO 22/10/19.
78. RUSI, *A Democratic Licence to Operate*, 111-14; see IPCO Ann Rept 2017 para 2.11 for Fulford justification.
79. Members of expert bodies may also hear appeals against refusals of security clearance, e.g., NSIRA in Canada and chairs of Committees I and P sit with head of Data Protection Commission in Belgium (Laethem, 2018, 109). CTIVD now divides responsibility of its members between hearing public complaints and conducting oversight (2019, 9).
80. Petersen & Tjalve, "Intelligence Expertise in the Age of Information Sharing," 22
81. The 2019 documentary film 'The Great Hack' shows part of a Cambridge Analytica presentation by (later) whistleblower Bethany Kaiser in which she claimed: 'we are a behaviour-change agency'. https://www.netflix.com/gb/title/80117542
82. 'It is in the nature on instrumentarian power to operate remotely and move in stealth. It does not grow through terror, murder, the suspension of democratic institutions, massacre or expulsion. Instead, it grows through declaration, self-authorization, rhetorical misdirection, euphemism, and the quiet, audacious backstage moves specifically crafted to elude awareness as it replaces individual freedom with others' knowledge and *replaces society with certainty*. It does not confront democracy but rather erodes it from within, eating away at the human capabilities and self-understanding required to sustain a democratic life.' Zuboff, *The Age of Surveillance Capitalism*, 381, emphasis added.

83. Zuboff, *The Age of Surveillance Capitalism*, 385
84. Fry & Hochstein, "Epistemic Communities"; Gill & Phythian, *Intelligence in an Insecure World*, 45-66.
85. Petersen & Tjalve, "Intelligence Expertise in the Age of Information Sharing," 23.
86. Gill, *Intelligence Governance and Democratisation*, 69; also Petersen & Tjalve, "Intelligence Expertise in the Age of Information Sharing," 25.
87. Gill, *Intelligence Governance and Democratisation*, 67-74.
88. Zuboff, *The Age of Surveillance Capitalism*, 112-21 quote at 115.
89. Zuboff, *The Age of Surveillance Capitalism*, 377 and see 504-12 re. 'radical indifference'
90. cf. Treverton, Theory and Practice.
91. Open Rights Group, 2019.
92. Wetzling & Vieth, *Upping the Ante on Bulk Surveillance*, esp 21-82
93. Van Laethem, "The Rule of Law and 25 Years of Intelligence Oversight in an Ever-Changing World," 106.
94. CTIVD, *Annual Report for 2019*.
95. Wetzling & Vieth, *Upping the Ante on Bulk Surveillance*, 84-85; cf. Quarmby, *Intelligence in Regulation*, 39-43.
96. Vieth & Wetzling, "Data-driven Intelligence Oversight."
97. van Buuren, "From Oversight to Undersight," 244-46; cf. Zuboff, *The Age of Surveillance Capitalism*.
98. Lefebvre, "The Difficulties and Dilemmas of International Intelligence Cooperation," 534-36.
99. CTIVD, *Annual Report for 2019*, 10
100. See O'Connor, "Report of the Commission of Inquiry."
101. McGruddy, "Multilateral Intelligence Collaboration and International Oversight," 220
102. Aldrich, "Global Intelligence Cooperation versus Accountability," 56.
103. Aden, "Information Sharing, Secrecy and Trust among Law Enforcement," 982.
104. De Ridder, "A Simple yet Existential Demand: Let Oversight Bodies Work Together."
105. CTIVD, *Annual Report for 2019*, 16-19.
106. https://ipco.org.uk/default.aspx.
107. CTIVD statement 14 November 2018.
108. IPCO, 2018.
109. Van Laethem, "The Rule of Law and 25 Years of Intelligence Oversight in an Ever-Changing World," 105
110. Moran, "The Rise of the Regulatory State."
111. Black, "Critical Reflections on Regulation," 8-9.
112. Quarmby, *Intelligence in Regulation*, 108-11.
113. van Puyvelde, *Outsourcing US Intelligence*.
114. https://small-firms.fca.org.uk/fees-and-levies.
115. Van Laethem, "The Rule of Law and 25 Years of Intelligence Oversight in an Ever-Changing World," 114
116. Loader & Walker, *Civilizing Security*.
117. cf. Aldrich & Richterova, "Ambient Accountability," 1005; van Buuren, "From Oversight to Undersight," 239.
118. Gill, *Intelligence Governance and Democratisation*, 210-14; van Buuren, "From Oversight to Undersight."
119. Wegge, "Intelligence Oversight and the Security of the State," 695.
120. P&T, 2018, 30.
121. Gill, "Inquiring into Dirty Wars."
122. Glaser, *Anti-Politics*.

Acknowledgements

Many thanks to Stuart Farson for his critique on an early draft of this article and to the journal's reviewers for their comments.

Disclosure statement

No potential conflict of interest was reported by the author.

Notes on contributor

Peter Gill was previously Professor of Politics and Security at Liverpool John Moores University (2004-2007) and Research Professor in Intelligence Studies at the University of Salford (2007-2009). He was honorary fellow at University of Liverpool 2009-2016 and University of Leicester 2016-2019. He wrote *Policing Politics* (Cass, 1994), *Rounding Up the Usual Suspects* (Ashgate, 2000) and *Intelligence Governance and Democratisation: a comparative analysis of the limits of reform* (Routledge, 2016). He has also co-authored *Intelligence in an Insecure World* (3rd edition, Polity,

2018) and *Democratization of Intelligence* (Routledge, 2015).

Bibliography

Aden, H. "Information Sharing, Secrecy and Trust among Law Enforcement and Secret Service Institutions in the European Union." *West European Politics* 41, no. 4 (2018): 981–1002. doi:10.1080/01402382.2018.1475613.

Agrell, W., and G. F. Treverton. *National Intelligence and Science: Beyond the Great Divide in Analysis and Policy*. Oxford: Oxford UP, 2015.

Aldrich, R. "Global Intelligence Cooperation versus Accountability: New Facets to an Old Problem." *Intelligence and National Security* 24, no. 1 (2009): 26–56. doi:10.1080/02684520902756812.

Aldrich, R., and D. Richterova. "Ambient Accountability: Intelligence Services in Europe and the Decline of State Secrecy." *West European Politics* 41, no. 4 (2018): 1003–1024. doi:10.1080/01402382.2017.1415780.

Anderson, D. 2015. "A Matter of Trust." https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf

Black, J. 2002. "Critical Reflections on Regulation." *Australian Journal of Legal Philosophy* 27: 1–33.

Born, H., L. Johnson, and I. Leigh. *Who's Watching the Spies: Establishing Intelligence Service Accountability*. Dulles: Potomac Books, 2005.

Bowcott, O. 2019. "Court Told MI5 Kept Material and Gained Warrants Illegally." *The Guardian*, June 12, 10.

Caparini, M. "Comparing the Democratisation of Intelligence Governance in East Central Europe and the Balkans." *Intelligence and National Security* 29, no. 4 (2014): 498–522. doi:10.1080/02684527.2014.915175.

Cayford, M., W. Pieters, and C. Hijzen. "Plots, Murders, and Money: Oversight Bodies Evaluating the Effectiveness of Surveillance Technology." *Intelligence and National Security* 33, no. 7 (2018): 999–1021. doi:10.1080/02684527.2018.1487159.

Colaresi, M. *Democracy Declassified: The Secrecy Dilemma in National Security*. Oxford: Oxford UP, 2014.

Corfield, G. 2019. "MI5 Slapped on the Wrist for "Serious" Surveillance Data Breach." *The Register*, May 15.

CTIVD, 2018. Joint Statement: *Strengthening Intelligence Oversight Cooperation*, November 14.

CTIVD. 2019. *Annual Report for 2018*.

D.C. McDonald. "Commission of Enquiry Concerning Certain Activities of the Royal Canadian Mounted Police." Second Report: *Freedom and Security under the Law*, Ottawa: Minister of Supply and Service, 1981.

de Ridder, W. 2019. "A Simple yet Existential Demand: Let Oversight Bodies Work Together." *About:Intel*, November. https://aboutintel.eu/simple-oversight-demands/

Dietrich, J.-H. "Of Toothless Windbags, Blind Guardians and Blunt Swords: The Ongoing Controversy about the Reform of Intelligence Services Oversight in Germany." *Intelligence and National Security* 31, no. 3 (2016): 397–415. doi:10.1080/02684527.2015.1017246.

Dobson, M. "The Last Forum of Accountability? State Secrecy, Intelligence and Freedom of Information in the United Kingdom." *British Journal of Politics and International Relations* 21, no. 2 (2019): 312–329. doi:10.1177/1369148118806125.

Edelman, M. *The Symbolic Uses of Politics*. Urbana: University of Illinois Press, 1985. (orig. published 1964).

Eskens, S., O. van Daalen, and N. van Eijk, *Ten standards for oversight and transparency of national intelligence services*, Institute for Information Law, University of Amsterdam, 2015 www.ivir.nl

Farson, S., and R. Whitaker. "Accounting for the Future or the Past?: Developing Accountability and Oversight Systems to Meet Future Intelligence Needs." In *The Oxford Handbook of National Security Intelligence*, edited by Loch Johnson, 673–698. Oxford: Oxford UP, 2010.

Frank Church. 1976. *Final Report of the Select Committee to study Governmental Operations with respect to Intelligence Activities*, United States Senate, Book 1. https://www.intelligence.senate.gov/resources/intelligecne-related-commissions

Fry, M. G., and M. Hochstein. "Epistemic Communities: Intelligence Studies and International Relations." *Intelligence and National Security* 8, no. 3 (1993): 14–28. doi:10.1080/02684529308432212.

Fuior, T. "Romania's Experience of Intelligence Oversight." In edited by Leigh and Wegge, 57–74. 2018.

Gill, P. *Policing Politics: Security Intelligence and the Liberal Democratic State*. London: Frank Cass, 1994.

Gill, P. "The Intelligence and Security Committee and the Challenge of Security Networks." *Review of International Studies* 35, no. 4 (2009): 929–941. doi:10.1017/S0260210509990362.

Gill, P. "Inquiring into Dirty Wars: A 'Huge Smokescreen of Humbug'?" In *Commissions of Inquiry and National Security*, edited by S. Farson and M. Phythian, 78–97. Santa Barbara: Praeger, 2011.

Gill, P. "Intelligence, Threat, Risk and the Challenge of Oversight." *Intelligence and National Security* 27, no. 2 (2012): 206–222. doi:10.1080/02684527.2012.661643.

Gill, P. *Intelligence Governance and Democratisation: A Comparative Analysis of the Limits of Reform*. Abingdon: Routledge, 2016.

Gill, P., and M. Phythian. *Intelligence in an Insecure World*. 3rd ed. Cambridge: Polity, 2018.

Glaser, E. *Anti-Politics: On the Demonization of Ideology, Authority and the State*. London: Repeater Books, 2018.

Hastedt, G. "The Politics of Intelligence Accountability." In *The Oxford Handbook of National Security Intelligence*, edited by L. Johnson, 719–734. Oxford: Oxford UP, 2010.
Hegemann, H. "Toward 'Normal' Politics? Security, Parliaments and the Politicisation of Intelligence Oversight in the German Bundestag." *British Journal of Politics and International Relations* 20, no. 1 (2018): 175–190. (pdf in/articles). doi:10.1177/1369148117745683.
Hennessy, P. "From Secret State to Protective State." In *The New Protective State: Government, Intelligence and Terrorism*, edited by Hennessy, 1–41. London: Continuum, 2007.
Hijzen, C. "More than a Ritual Dance. The Dutch Practice of Parliamentary Oversight and Control of the Intelligence Community." *Security and Human Rights* 24 (2013): 227–238. doi:10.1163/18750230-02404002.
Hillebrand, C. "Intelligence Oversight and Accountability." In *Routledge Companion to Intelligence Studies*, Robert Dover, Michael Goodman & Claudia Hillebrand edited by, 305–312. 2013. Abingdon: Routledge.
Intelligence Services Commissioner. 2016. "Supplementary to the Annual Report for 2015, HC458, Para.6.15." September 15. http://www.intelligencecommissioner.com/docs/FPCM1042_HC_458_Accessible.pdf
IPCO. 2018. https://ipco.org.uk/docs/IPCO%20Statement%20re%205%20oversight%20bodies.docx
ISC. 2006. "*Report into the London Terrorist Attacks on 7 July 2005* Cm 6785". http://isc.independent.gov.uk/committee-reports/special-reports,
ISC. 2018. *Diversity and Inclusion in the UK Intelligence Community*, HC1297. July 18. http://isc.independent.gov.uk/committee-reports/special-reports
ISC. *Could 7/7 Have Been Prevented?* Cm 7617, 2009, para.11. http://isc.independent.gov.uk/committee-reports/special-reports
Kibbe, J. "Congressional Oversight of Intelligence: Is the Solution Part of the Problem?" *Intelligence and National Security* 25, no. 1 (2010): 24–49. doi:10.1080/02684521003588104.
Laethem, W. V. "Parliamentary and Specialized Oversight of Security and Intelligence Agencies in Belgium." *Parliamentary Oversight of Security and Intelligence Agencies in the EU*, Director-General of Internal Policies, pp. 191–203. Brussels: European Parliament, 2011.
Lefebvre, S. "The Difficulties and Dilemmas of International Intelligence Cooperation." *International Journal of Intelligence and CounterIntelligence* 16, no. 4 (2003): 527–542. doi:10.1080/716100467.
Leigh, I. "Reappraising Intelligence Oversight in the UK." In edited by Leigh and Wegge, 78–95. 2018.
Leigh, I., and N. Wegge, eds.. *Intelligence Oversight in the Twenty-First Century: Accountability in a Changing World*. Abingdon: Routledge, 2018.
Lester, G. *When Should State Secrets Stay Secret? Accountability, Democratic Governance, and Intelligence*. Cambridge: Cambridge UP, 2015.
Loader, I., and C. Walker. *Civilizing Security*. Cambridge: Cambridge UP, 2007.
McGruddy, J. "Multilateral Intelligence Collaboration and International Oversight." *Journal of Strategic Security* 6, no. 3 (2013): 214–220. Fall. doi:10.5038/1944-0472.6.3S.22.
McLaughlin, J. 2018. "Lawmakers Demand Investigation into Lack of Whistleblower Protections for Spies." *Foreign Policy*, January 18.
Moran, M. "The Rise of the Regulatory State." In *The Oxford Handbook of Business and Government*, edited by D. Coen, W. Grant, and G. Wilson, 383–403. Oxford: Oxford UP, 2010.
O'Connor, D. 2006. "Report of the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar." https://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.ararcommission.ca/eng/index.htm
Omand, D. 2010. *Securing the State*. London: Hurst & Co.
Open Rights Group. 2019. "KARMA POLICE: UK Mass Surveillance Challenge Will Go to Europe's Highest Human Rights Court." February 6.
Otamendi, A., and E. Estévez. "Intelligence Challenges in Latin America and Prospects for Reform: A Comparative Matrix on Democratic Governance." In *Nevos Paradigmas de la vigilancia? Miradas desde América Latina*, edited by C. Rios, 277–294. Buenos Aires: Lavits, 2017.
Pejic, J. 2018. "Proper Constitution Is Necessary for Accountable Political Power." http://bezbednost.org/All-publications/6775/Proper-Constituiojn-is-Necessary-for-Accountable.shtml
Petersen, K. L., and V. S. Tjalve. "Intelligence Expertise in the Age of Information Sharing: Public–private 'Collection' and Its Challenges to Democratic Control and Accountability." *Intelligence and National Security* 33, no. 1 (2018): 21–35. doi:10.1080/02684527.2017.1316956.
Petrovic, P. "Serbia." In *The Handbook of European Intelligence Cultures*, edited by B. de Graaff and J. M. Nyce, 321–333. Lanham: Rowman & Littlefield, 2016.
Quarmby, N. *Intelligence in Regulation*. Annandale: The Federation Press, 2018.
Rittberger, B., and K. H. Goetz. "Secrecy in Europe." *West European Politics* 41, no. 4 (2018): 825–845. doi:10.1080/01402382.2017.1423456.
RUSI. 2015. *A Democratic Licence to Operate*, July, 111–114 https://rusi.org/sites/default/files/20150714_whr_2-15_a_democratic_licence_to_operate.pdf
Savage, C. 2019. "We Just Got a Rare Look at National Security Surveillance. It Was Ugly." *New York Times*, December 11.

Savage, C. 2020. "Inspector General Fired by Trump Urges Whistle-blowers "To Bravely Speak Up"." *New York Times*, April 6. https://www.nytimes.com/2020/04/06/us/politics/michael-atkinson-inspector-general-fired.html

Treverton, G. F. "Theory and Practice." In *Developing Intelligence Theory: New Challenges and Competing Perspectives*, edited by M. Gill, 6–12. Phythian ed. Abingdon: Routledge, 2019.

Van Buuren, J. "From Oversight to Undersight: The Internationalization of Intelligence." *Security and Human Rights* 24, no. 3–4 (2013): 239–252. doi:10.1163/18750230-02404003.

van Laethem, W. "The Rule of Law and 25 Years of Intelligence Oversight in an Ever-Changing World: The Belgian Case." In edited by Leigh and Wegge, 97–123. 2018.

van Puyvelde, D. *Outsourcing US Intelligence: Contractors and Government Accountability*. Edinburgh: Edinburgh University Press, 2019.

Venice Commission, 2015. *Report on the Democratic Oversight of the Security Services*, December 15. Studies no. 388/2006 and 719/2013.

Vieth, K., and T. Wetzling. 2019. "Data-driven Intelligence Oversight: Recommendations for a System Update." *Stiftung Neue Verantwortung*, November.

Warusfel, B. "The Intensification of French Intelligence and Its Oversight under the Impact of Counter-terrorism." In edited by Leigh and Wegge, 124–134. 2018.

Wegge, N. "Intelligence Oversight and the Security of the State." *International Journal of Intelligence and Counterintelligence* 30 (2017): 687–700. doi:10.1080/08850607.2017.1337445.

Wetzling, T. "Intelligence Governance in Post-Cold War Germany: A Steady Beat of Constant Trouble?" In edited by Leigh and Wegge, 170–189. 2018.

Wetzling, T., and K. Vieth. *Upping the Ante on Bulk Surveillance: An International Compendium of Good Legal Safeguards and Oversight Innovations*. Publication Series on Democracy, Volume 50. Berlin: Heinrich Bőll Stiftung, 2018.

Wills, A. *Guidebook: Understanding Intelligence Oversight*. Geneva: DCAF, 2010.

Wills, A., and H. Born. "International Intelligence Cooperation and Accountability: Formidable Challenges and Imperfect Solutions." In *International Intelligence Cooperation and Accountability*, edited by L. Born and Wills, 277–308. Abingdon: Routledge, 2011.

Zegart, A. B., and J. Quinn. "Congressional Intelligence Oversight: The Electoral Disconnection." *Intelligence and National Security* 25, no. 6 (2010): 744–766. doi:10.1080/02684527.2010.537871.

Zuboff, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books, 2019.

Zulean, M., and E. Şercan. 2018. "Democratic Control of Romanian Intelligence after Three Decades: Quis Custodiet Ipsos Custodes?" *Defense and Security Analysis*. online, 1020.