Policing & Society
Vol. 22, No. 2, June 2012, 133–151

Making up 'Terror Identities': security intelligence, Canada's Integrated Threat Assessment Centre and social movement suppression

Jeffrey Monaghan[a] and Kevin Walby[b]*

[a]*Department of Sociology, D431 Mackintosh-Corry, Queen's University, Kingston, ON K7L 3N6, Canada;* [b]*Department of Sociology, University of Victoria, PO Box 3050 STN CSC, Cor A333, 3800 Finnerty Rd., Victoria, BC V8W 3P5, Canada*

(*Received 11 October 2010; final version received 16 March 2011*)

Drawing on analysis of government records obtained using *Access to Information Act* (ATIA) requests, we examine policing and surveillance projects developed in preparation for three mega-events that recently took place in Canada – the 2010 Winter Olympics, the G8/G20 meetings and a scheduled (but cancelled) North American Leaders Summit. Based on an investigation of 'Threat Assessment' reports produced between 2005 and 2010 by the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS), we discuss transformations within Canada's anti-terror intelligence networks including the establishment of Integrated Security Units (ISUs) and the Integrated Threat Assessment Centre (ITAC) which resemble intelligence 'fusion centers' in the United States. These organisations became the knowledge-producing hubs for the classification and categorisation of national security threats. Examining shifts in ISU and ITAC Threat Assessments, we demonstrate how knowledge construction practices in security intelligence networks produce new categories of threat. Specifically, we focus on the newly constructed notion of 'multi issue extremism' (MIEs). Exploring the deployment of MIEs as a category of national security threat, we show how intelligence agencies have blurred the categories of terrorism, extremism and activism into an aggregate threat matrix.

Keywords: security; intelligence; anti-terrorism policing; threat assessments; social movements

Introduction

Recent literature on surveillance and social movements has described the spectacle of surveillance around mega-events such as the Olympic Games (Boyle and Haggerty 2009) and has discussed trends concerning the integration of policing, security and intelligence agencies (see Manning 2006, de Lint and Hall 2009, Monahan and Palmer 2009). Yet, little research has explored the fusion of intelligence agencies in Canada. Nor has much research investigated how security intelligence agencies construct the categories that they use to categorise and classify threats. Below, we investigate trends concerning security intelligence in Canada and the transformations made in preparation for three major events held in the year 2010: the ratification meetings for a North American security pact known as the Security and Prosperity Partnership,[1] the Winter Olympics in Vancouver/Whistler, British Columbia and the

*Corresponding author. Email: 11jmrm@queensu.ca

ISSN 1043-9463 print/ISSN 1477-2728 online
© 2012 Taylor & Francis
http://dx.doi.org/10.1080/10439463.2011.605131
http://www.tandfonline.com

G8/G20 meetings in Huntsville/Toronto, Ontario. Leading up to these events, the Canadian security establishment underwent a significant transformation to address perceived national security threats.

Using requests under the *Access to Information Act* (ATIA), we have collected 25 classified reports from the intelligence branch of Canada's national police, the Royal Canadian Mounted Police (RCMP), as well as from the national intelligence service, Canadian Security Intelligence Service (CSIS). These 'Threat Assessment' reports detail domestic terrorism threats spanning from 2005 to 2010. Below we discuss how the formation of the Integrated Security Unit (ISU) in response to the mega-events of 2010 centralises policing and intelligence functions, fusing together municipal police, regional/provincial police, the RCMP, CSIS, as well as the Canadian military. ISUs are unprecedented multi-agency amalgams for domestic security, with only two having been established in Canada: one ISU for the Vancouver-based Olympic Games and another for the G8/G20. Major federal agencies – particularly the RCMP, CSIS, and the Department of National Defence – are the central actors in both ISUs.[2] The substantive focus of intelligence from 2005 onward was the 2010 Olympics Games, and therefore our data reflect the centrality of the Games for 2010 security coordination across Canada.[3] The Threat Assessments were produced from sources including local police, national security and intelligence agencies, international allies and media reports. Prior to 2007, these Threat Assessments were undertaken by numerous policing and intelligence agencies. However, in 2007, the responsibility for coordinating security intelligence was passed to CSIS's newly formed Integrated Threat Assessment Centre (ITAC). Our examination of the subsequent reports coordinated under the leadership of ITAC reveals a transformation in the substantive content of anti-terror intelligence and also the categories through which national security intelligence is produced in Canada.

Beyond focusing on the integration of policing, security and intelligence agencies, we discuss the production of threat categories and the knowledge construction practices that special intelligence clusters engage in. We focus on a newly produced category of security threat: Multi Issue Extremism, or MIEs. The emergence of MIEs as a category of domestic terrorism signals two broad transformations. The first transformation concerns a significant shift in perceived threats. Early intelligence briefs are concerned with financial security and Al-Qaeda-inspired terror groups. However, ITAC-coordinated Threat Assessments expand their focus to target MIEs, described as activist groups, indigenous groups, environmentalists and others who are publicly critical of government policy. The second trend concerns slippages and inconsistencies of threat categories in ITAC reports. Specifically, intelligence agencies have blurred the categories of terrorism, extremism and activism into an aggregate threat matrix. This blurring of threat categories expands the purview of security intelligence agencies, leading to net-widening where a greater diversity of actions are governed through surveillance processes and criminal law. Given the scale and depth of security measures taken in preparation for the 2010 mega-events, the repercussions for security intelligence are structural and long term.[4]

By demonstrating how networks of policing, security and intelligence agencies communicate about activist groups who are classified as a threat to public order, we contribute to literature on security intelligence and also literature on social movements. Cunningham (2004) argues that scholarship on social movement repression does not account for the multiple scales of police involved in repression.

In addition, the term 'repression' emphasises overt coercive practices instead of clandestine surveillance practices that are better referred to as 'suppression' (see Boykoff 2007). Thus, we analyse how the ISU and ITAC create a network of policing, security and intelligence agencies in Canada, casting a wider net of surveillance that aims to pre-emptively regulate ostensible national security threats. Our analysis supplements research on intelligence fusion centres in the USA (see Monahan and Palmer 2009, Newkirk 2010) by showing that the ISU and ITAC in Canada provide a site for policing, security and intelligence agencies to be networked through surveillance. We also explore the work that intelligence agents do in creating what we call 'terror identities'. Our analysis thus supplements the work of Boyle and Haggerty (2009) by arguing that though the spectacle of security surrounding mega-events is key, material practices of securitisation must be empirically explored as they are not necessarily reducible to the spectacle; social movement suppression aims to compose a picture in which political opposition is removed from the frame.

This article is organised in four parts. First, we conceptualise how policing, security and intelligence agencies are networked through surveillance in Canada. We also discuss security intelligence and surveillance in relation to social movement suppression. Second, we discuss the implications of using the ATIA for conducting research on policing, security and intelligence agencies. Third, we discuss the formation of intelligence clusters in Canada as it concerns preparations for the 2010 Games. Focusing on the emergence of MIEs as a prominent 'national security' concern, we discuss how these intelligence clusters engage in construction of 'terror identities'. We conclude by discussing issues concerning surveillance, security and social movement suppression.

Security intelligence, Integrated Security Units (ISUs) and Joint Intelligence Groups (JIGs)

Signals intelligence, or SIGNIT, refers to intelligence compiled through the interception of communications, which differs from human intelligence, or HUMINT, referring to intelligence derived from a human source through infiltration or interrogation (which may or may not involve torture). Despite widespread adoption of information and communication technologies by intelligence agencies for the purposes of penetrating deeper into SIGNIT, HUMINT gathered through infiltration is still heavily used by security intelligence agencies and the policing agencies that feed information into intelligence networks (see Brodeur and Dupont 2006). The 'security' of 'security intelligence' eludes a firm definition, insofar as 'security' is an organising metaphor that directs policing and order maintenance activities (Neocleous 2008).

Lippert and O'Connor (2006, p. 53) usefully define 'security intelligence' as a 'process that includes coercive or covert acquisition of data about security issues, events and responses'. Attempts to achieve order maintenance through 'security' are best defined as a process with material consequences (Bigo 2002), which would require security and policing studies to move beyond empirical restrictions that come from focusing solely on the speech acts of politicians. 'Security preparedness' has become an institutionalised governmental paradigm, and efforts at securitisation require the cooperation of numerous policing, security, intelligence and military agencies (Deflem 2004, Dupont 2004). Efforts at securitisation also require classifications and categories provided and created by intelligence reports.

Security intelligence has conventionally been the domain of national or federal-level governments, developing later in Canada than in the United Kingdom and the United States (Gill 2006). However, in all three countries, there has been a recent transformation of security intelligence. This transformation includes a broadening of the scope and a 'fusion' of the responsibility for security intelligence, primarily in response to the perceived failures of intelligence with the events of 11 September 2001. The 'doctrinal changes' (Gill 2004) or 'mission adaptation' (Deukmedjian and de Lint 2007) are altering the face of security intelligence in Canada. Bell (2006) argues that, since 11 September 2001, national security and intelligence agencies in Canada have explicitly extended their reach, where the targets are defined more on the basis of suspicion.[5] This development breaks from the 'good governance' paradigm of security intelligence during earlier decades (see Jensen 2009).

In preparation for the 2010 mega-events, Canadian policing agencies centralised security-intelligence preparations by creating the Integrated Security Unit (ISU). In 2003, the Vancouver ISU became the de facto policing-security hub for the upcoming mega-events, particularly after it was announced that the G8/G20 would be held in Toronto.[6] Under the command structure of the RCMP, the ISU consisted of approximately 15,500 police from 120 police and law enforcement agencies across Canada. The ISU also included thousands of members of the Canadian armed forces and private security personnel. It was tasked with coordinating security with international allies, mostly the United States and NORAD.[7] The initial intelligence functions of the ISU were primarily assigned to its Joint Intelligence Group, or JIG. While the ISU-JIG was a creation of the RCMP, its composition included municipal and provincial police, the Canadian armed forces and CSIS. JIG issued its first 'preliminary' Threat Assessment related to the 2010 mega-events on 12 May 2005. Later, in a report from 1 April 2007, the JIG's function is described as follows: 'The JIG plans to develop a comprehensive public order portfolio to monitor and access high risk groups, individuals, and potential threats to Olympic-related events'. From its inception in 2005 until the 2010 mega-events, the JIG played a central role in coordinating security intelligence practices. Notably, however, after meetings in late 2006, it was decided that the editorial control of 'Threat Assessments' would be undertaken by a CSIS agency, known as the Integrated Threat Assessment Centre (ITAC).

The centralisation of intelligence under the ISU-JIG (and later ITAC) in Canada resembles Department of Homeland Security 'fusion centres' in the United States, which coordinate data-sharing among state and local police, intelligence agencies and private companies. Fusion centres involve both centralisation and extension of intelligence practices: coordination is concentrated in a few, new agencies, but intelligence gathering responsibilities are extended to local and regional police who never before participated in such networks (Newkirk 2010). Fusion centres are often subject to what Monahan and Palmer (2009, p. 620) call 'mission creep' where the functions of fusion centres 'expand beyond their originally intended purposes to encompass all perceive threats and hazards'. Mission creep within Canadian agencies was extensive and, over five years, transformed from abstract concerns around Al-Qaeda terrorist groups to intensive surveillance of political opponents that publicly criticised a myriad of issues associated with hosting the Olympic Games. The ISU-JIG and ITAC resemble fusion centres in the United States, though the bureaucratic character of these agencies – as well as a significant difference in scale – prevents any total fusion (see Deflem 2004). A longstanding animosity between the RCMP and CSIS also shapes Canada's security intelligence field.

'Mission creep' happens in response to on-the-ground intelligence produced by investigative practices focused on prominent opposition groups. In Canada, ISU 'mission creep' resulted in the cataloguing of many left-wing associated groups as threatening, particularly those associated with direct action tactics. Fernandez (2008) notes the now common practice of coding political opposition through the lens of 'crime control' and, in the context of the Olympics, this practice became an initial platform on which intelligence agencies constructed security threats (see also Manning 2006).

Opposition to the Games was rooted in a number of contentious issues, aggravated by the astounding costs of hosting mega-events. As the 2010 Games in Vancouver approached, the ISU became aware that domestic opposition was the most likely potential disruption and undertook a number of suppression operations to disrupt anti-Olympic movements. Boykoff (2007, p. 12) describes 'suppression' as 'a process through which the preconditions for dissident action, mobilisation, and collective organisation are inhibited by either raising their costs or minimising their benefits'. The use of the term 'suppression' is more accurate than the term 'repression' because our focus is not the 2010 mass mobilisations against the Olympics (or G8/G20) but instead the multiple-year preparatory campaigns that were opposed to many issues related to hosting the Olympics.

Suppression tactics are subtle forms of de-mobilisation. When based on HUMINT, suppression can take the form of 'inductive surveillance' (Brodeur and Leman-Langlois 2006) which is infiltration based on proximity to a target. For example, ISU officers made numerous house-calls to prominent activists and critics before the Olympics. Between 3 and 5 June 2009, approximately 15 anti-Olympics activists were visited by approximately eight ISU members. The ISU also had covert officers that spent several years undercover with groups in British Columbia and Ontario.[8] There is one instance where an undercover Vancouver police officer attended a 2009 public event in Hamilton to gather information on a prominent anti-Olympic activist during a speaking tour of Ontario and Québec. Our use of the term 'suppression' signals these on-going projects of surveillance that are aimed at deterring movement participation through police harassment and possible criminalisation. This includes mechanisms by which policing and intelligence agencies try 'to squelch dissent' (Boykoff 2007, p. 314), often using knowledge accrued through surveillance, which lays the framework for future police monitoring, raids, and criminalisation of activists.[9]

Knowledge of perceived threats determines the character of policing practices, since knowledge construction practices inform organisational responses to different threats. Acting as fusion centres, the ISU-JIG and ITAC produce categories that are used in subsequent intelligence reports and may be applied in local policing contexts. As Bowker and Star (1999, p. 3) argue, categories provide an 'organizing rubric' for policing agencies, and these categories play an important role in ordering human conduct. Categories in part *make up* the object of knowledge construction and regulation. The construction of threat in intelligence reports is not always based on 'facts' but can stem from claims found in previous intelligence reports or that are introduced by intelligence agents and then circulated to other agencies (Innes *et al.* 2005, Daase and Kessler 2007). Through circulation within policing, security, and intelligence agencies, as well as the mass media (see Boyle and Haggerty 2009), claims about threat take on a facticity (see Innes *et al.* 2005). Thus, we focus on how intelligence clusters create what we refer to as 'terror identities'. We use the idea of 'terror identities' to signal how contentious collective action is subject to the labelling and classification practices of intelligence agencies.

Method and access to information

Due to the enigmatic character of national security, it is difficult to conduct interviews with intelligence officers about their work (Marx 1984, Earl 2009). Thus, we use access to information (ATI) requests as part of a methodological strategy for tracing transformations within Canadian security intelligence. In Canada, scholars have increasingly utilised the *Access to Information Act* (ATIA) as a methodological tool to conduct research on policing, security and intelligence practices (see Larsen and Piché 2009, Walby 2009, Piché and Walby 2010, Walby and Monaghan 2010, 2011, Walby and Lippert forthcoming, Walby and Larsen forthcoming). ATI research has been used to detail police practices. For instance, Gentile and Kinsman (2009) have used ATI to document the multiple-decade surveillance and disruption campaign directed against the queer liberation movement. Similarly, the RCMP's surveillance of the 1970 Vancouver Women's Caucus Abortion Caravan has been recently accessed (Sethna and Hewitt 2009).

The depths of information accessed through the ATIA can be remarkable, yet researchers continue to encounter stonewalling. These difficulties in using the ATIA demonstrates what Marx (1984) explained as the government's unwillingness to release 'dirty data' on contentious issues. Due to redactions, delays, as well as problems such as chronic under-funding of ATI branches (see Roberts 2006), ATIA users are aware that these requests rarely lead to full-picture explanations. However, disclosures can be combined to reveal policing and intelligence trends. ATI requests also allow a way of collecting data when it is not possible to conduct interviews, which is the case with RCMP and CSIS security intelligence officers in Canada.

Our ATIA requests focus on the RCMP and CSIS Threat Assessments that contained references to domestic extremism or use of the term 'multi issue extremism'. We obtained 25 intelligence reports that cover the period from 12 May 2005 to 19 January 2010. The intelligence for the reports was produced by numerous sources. As one ISU document puts it, the data included in intelligence reports are obtained 'from investigations, open source reports and law enforcement sensitive documents'. Reflective of the limits of ATI research, we have been unable to collect data on how many reports our data represent in the total number of reports produced, as asking for all occurrence reports would be too costly and would require years of consultation with all of the other agencies who contributed. Using ATI requests to produce data is limited when multiple government agencies are involved, since all agencies need to review and sign off on the disclosure before release. Although we are unable to discern the total number of 'Threat Assessments' produced, and the RCMP and CSIS do not disclose this sort of aggregate data, the period under examination spans the initial 'Preliminary Threat Assessment' produced by the ISU-JIG immediately before the Winter Olympics in Vancouver. These Threat Assessments appear under a number of names, since the intelligence products evolved over the time span. We received reports from the ISU-JIG, the

RCMP's National Security Threat Assessment Section (NSTAS), CSIS, as well as those from ITAC. Materials included in these reports are also gathered from the Canadian military (Department of National Defence and the Canadian Forces), and international allies. ITAC and the ISU also send intelligence reports 'to international partners (such as the Australians, UK and US)' as one report puts it (on transnational policing, see Sheptycki 1998).

The RCMP and CSIS were aware of the potential for people to access sensitive documents using the ATIA. Concealing information about Olympics-related intelligence and surveillance practices was of particular concern. In a Situation Report for the RCMP dated 1 April 2007, the ISU-JIG details the potential of ATIA in the following terms:

> Access to Information and Privacy (A-TIP) can adversely affect the security of the Games. Recent A-TIP requests to the 2010 Integrated Security Unit (ISU) has worked to publicize 2010 ISU-JIG capabilities, vulnerabilities and resources. Such information can be put to nefarious counter-intelligence use by terrorist or protest groups compromising the security of the 2010 Games.[10]

The ISU-JIG proposes that the RCMP lobby political leaders to add an exemption for their activities. The report concludes:

> Special A-TIP exemption should be sought to defer requests to at least two years after the 2010 Games. The temporary exemption would help ensure that the integrity of Games security was maintained. The public's requirement for government transparency should be tempered with concerns for national security and safety by protecting information which could otherwise be used for counter-intelligence or other nefarious purposes.

These cautions are suggestive of how important ATI can be in accessing 'dirty data' and the lengths that policing, security and intelligence agencies go to bury traces of their work. To our knowledge, neither the RCMP nor any other agency received ATIP exemptions. Notwithstanding these objections, material considered to be sensitive can be redacted and omitted from ATIP disclosures (Roberts 2006, Walby and Larsen forthcoming) and, as is common with ATI requests on policing and security matters, many of the documents we accessed have been redacted.

Creating an intelligence cluster: the Integrated Threat Assessment Centre

The Vancouver Winter Olympics were subject to widespread opposition and resistance (Shaw 2008, Boykoff 2011). Opponents included anti-poverty activists, taxpayer groups and environmental coalitions. Gradually, a substantial part of the resistance movement became organised by indigenous and indigenous solidarity groups under the banner of 'No Olympics on Stolen Native Land' (O'Bonsawin 2009), since the planned Olympic zone was almost entirely unceded territory. The symbolism of the corporate-dominated Olympics was an iconic expression of the colonial present, above all because of the Olympics organising committee's attempts to co-opt indigenous imagery for marketing purposes.

The Olympics are among a select number of global mega-events, which includes the World Cup, other global sports competitions and political summits. As prominent public spectacles, the assumption that terrorists will strike these events has dominated governmental policies of preparedness, resulting in a precautionary logic of security (Roche 2000, Voulgarakis 2005, Manning 2006, Tsoulaka 2006). Indeed, Boyle and Haggerty (2009, p. 260) have noted that the spectacularity of the Olympics as a global mega-event prompts 'new processes of securitization where surveillance figures prominently'.

Precautionary security preparations for the Olympics were initially coordinated by the ISU, where the JIG was its primary surveillance and intelligence hub. However, during a 22 September 2006 meeting between leading branches of the Canadian security complex, the ISU tasked an agency named the Integrated Threat Assessment Centre (ITAC) with the task of centralising all national security-related intelligence distribution and coordination. Little is known about the ITAC. As a branch of CSIS, ITAC is governed by the *CSIS Act*. ITAC was created in October 2004 after the Canadian government issued its post-11 September 2001 national security policy, *Securing an Open Society: Canada's National Security Policy* (NSP). The function of ITAC is to act as a counter-terrorism intelligence hub and issue national security Threat Assessment reports. These assessments cover 'the ongoing threat to Canada from listed terrorist entities in Canada, and other ideologically motivated extremist entities active in Canada'. Prior to ITAC, no single federal organisation was responsible for analysing security intelligence or producing Threat Assessments.[11] The work of security intelligence was scattered among disparate agencies at the federal level, as well as provincial policing agencies in Ontario and Québec and even private security agencies (see Lippert and O'Connor 2006). An email from the RCMP Director General National Security, Al Nause, dated 24 October 2006, outlines the powers of the ITAC to act as the central agency for intelligence distribution. Nause writes:

> ITAC is comprised of several persons from different constituting agencies including the RCMP, CSIS, FAC, TC, Health Canada, CSC, and CBSA, etc... Each person, in our case the RCMP member on secondment, has access to their respective agency data banks; e.g., SPROS, SCIS etc... Because ITAC has the expertise and access to a wealth of information interdepartmentally and abroad, the RCMP as well as many other departments rely on ITAC to provide strategic threat assessments.[12]

The emergence of ITAC as a centralising hub of anti-terror intelligence in Canada in late 2006 is key for tracing the transformations in security intelligence preparations for the 2010 Olympic Games. Nause's email, detailing the 22 September meeting of Canada's security establishment leaders, claims that – despite other agencies still having responsibilities for their proper threat assessments – the ITAC will be 'responsible for preparing threats assessment for the government of Canada with respect to and *only* terrorism' (emphasis included).[13] ITAC emerges at this time as the principle authority over the identification and prioritisation of 'national security' threats, resulting in a transformation of the content of Threat Assessment reports. The signalled change rests in the final authorship and the ability of CSIS to frame issues according to their perception of potential threats. ITAC reports become the uppermost authority for categorising, framing and prioritising national security threats.

A principle shift of priorities in the national security Threat Assessment analysis from 2005 onward is the disappearance of 'financial security' as an area of concern. Several early Threat Assessments from the ISU-JIG stated that the main threat facing the Games were issues of commercial fraud and a range of property offences. For example, a 1 September 2006 report states: '[The] most probable and immediate security risk associated to the Vancouver 2010 Olympic and Paralympic Games is their financial security'. Though it is likely that financial fraud would decrease in risk after the completion of major infrastructure projects and awarding copyright and merchandising contracts, the shifting intelligence focus is illustrated by the initial concerns of the ISU towards social groups. While 'finance security' figured most prominently in early Threat Assessments, they also included notes concerning potential threats to 'public order' in the earliest reports. The most frequent reference to domestic protests speculate that major opposition will take the shape of anti-war demonstrations. These concerns proved to be incorrect. When the 2010 Games (and the G8/G20) arrived the on-going occupation of Afghanistan was among the least noticeable points of contention in Canada.

Early Threat Assessments contain numerous references to potential acts of terrorism. Much of the focus remains on groups such as Al-Qaeda, Hezbollah and the Tamil Tigers, with most references to these groups being cited from newspaper clippings and website searches. In earlier Threat Assessments, there are occasionally categorical distinctions between foreign and domestic terrorist threats. For instance, there are occasionally mentions of the so-called Toronto 18. At times, the Toronto 18 appears under a 'Domestic' category, however, in other reports it is listed under the category of terrorism. Early reports include only a short note that 'Protest activity is expected to increase as the international exposure grows'.

While early Threat Assessments are concerned with financial threats, Al-Qaeda and public health, over time, these Threat Assessments undergo a re-framing. On the ground, the diverse Olympic resistance movement began mobilising popular opposition to the Games. This opposition began to result in intelligence material gathered from various local policing agencies. ITAC began to re-code the diverse branches of the emerging movement against the Olympic Games in the discursive framework of 'extremism' and then 'terrorism'. Invoking language concerning 'critical public infrastructure' ITAC begins to shift focus from Al-Qaeda towards groups using direct action targets against corporate sponsors of the Olympics. What emerges are Threat Assessments with blurred threat categories, cataloguing a host of dissidents. The threat of terrorism comes to encompass an amalgam of grassroots opposition as a leading threat to the security of the Games and the public.

Making up 'Terror Identities': the emergence of multi issue extremism

According to one internal memo, the Threat Assessments produced by ITAC are modelled to address 'the ongoing threat to Canada from listed terrorist entities in Canada, and *other ideologically motivated extremist* entities active in Canada' (emphasis added). To include listed terrorist groups with any other ideologically motivated group casts a very wide net. This mandate coincides with a blurring of 'terrorism' and 'extremism' by ITAC. The construction of threat in intelligence agency reports often stems from organising rubrics found in previous intelligence reports, or sometimes are borrowed from news media (Daase and Kessler 2007).

Cold War intelligence reporting was straightforward. Today it is not as clear to these agencies who 'the enemy' is, which lends itself to the intelligence practice of creating classifications (Innes *et al.* 2005, de Lint 2008). In this way, the blurring of these categories has become a strategy of CSIS to rationalise domestic spying campaigns that target grassroots social movements under the statutory responsibilities of Canadian law. This shift constitutes what Deukmedjian and de Lint (2007) refer to as a 'mission adaptation' insofar as one set of intelligence targets disappears from the reports while grassroots political opposition receives more scrutiny. The shifting and blurred focus of these reports also draws attention to the knowledge work that intelligence officers do in creating the classifications that become organizing rubrics within intelligence clusters and the policing agencies they communicate with.

Central to the 'mission adaptation' undertaken by CSIS is its reconceptualisation of statutory powers. In a memorandum (with a redacted Subject line) prepared for the CSIS ADO, Charles Bisson, by the Director General of the AEA branch, explains how CSIS connects terrorism to domestic threats. The Memo states:

> Subsection 2 (a) of the *CSIS Act* identifies sabotage as one of the threats to the security of Canada which fall under the Service's investigational mandate. . .the *Act* speaks of 'sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such sabotage'.

The statutory definition provided seems vague, which is why Bisson, writing the memo, continues:

> Service policy OPS-100[14] defines activities 'detrimental to the interests of Canada' as those which would have a negative impact on Canada's national interests. 'Sabotage' is defined as activity 'conducted for the purpose of endangering the safety, security or defence of vital public or private property, such as installations, structures, equipment or systems'.

Here, CSIS twins the protection of domestic facilities and property with national interests. Aware of potential criticisms of the threat (or non-threat) of sabotage in the post-Cold War era, Bisson adds: 'At the time the *Act* was written, the threat of sabotage was perceived in the context of the Cold War as a threat emanating from foreign countries or agents and directed against the government of Canada'. In concert with other intelligence agencies' attempts to transition from state to non-state threats within the global War on Terror (see Berger and Borer 2007, Daase and Kessler 2007), this memo shows an interest in re-orienting the operational design of policing, security and intelligence practices toward 'security preparedness'. Unlike national security concerns towards non-state actors such as Al-Qaeda, though, this CSIS memorandum is focused on domestic threats, facilitated through creation of the classification 'multi issue extremism'.

The first reference to 'multi issue extremism' (MIEs) in the Canadian security complex stems from a 2007 CSIS report, released shortly after ITAC assumed responsibility for writing Threat Assessments.[15] The June 2007 internal CSIS report was titled 'Multi Issue Militancy'. However, that category quickly and consistently became 'extremism' in subsequent reports.[16] The June 2007 internal CSIS report states: 'As the Service positions itself for numerous events that could become targets of MIE groups, it is important that everyone be kept aware of the developments'. The report authored by CSIS also contains 'information volunteered by other governments, departments with a mandate related to, or an interest in, multi issue militancy'. The document catalogues a range of domestic protest activity, although it is impossible to reveal what forms of protest are contained in the redacted portions. However, under 'Potential Protests/upcoming activities', the only un-redacted mention is an upcoming meeting of NOWAR/PAIX in Ottawa, a local peace group comprised of mostly older, white pacifists. The document also has information related to global justice movement demonstrations in Europe, with a random mention of the use of an explosive in Greece. Under the 'National' heading, there is a note that the Sea Shepherd Conservation Society will sail under indigenous flags[17] and a description of a Yes Men stunt in Alberta.[18] Although the memo does not contain a working definition of MIEs, it spurs the widespread use of the term in subsequent Threat Assessments.

Less than a month later, on 20 July 2007, ITAC issues a Threat Assessment for the upcoming Security and Prosperity Partnership meetings in Montebello, Québec (which included a visit from George W. Bush). There is no reference to MIEs in previous reports, nor any other CSIS materials. But suddenly MIEs emerge as a central threat to Canadian interests. The report states:

> The principal security concern for the [leaders summit] will be the potential for violent protests by multi-issue extremists. A number of groups are actively organizing and planning protests in Montebello, Quebec and in Ottawa, Ontario.

In the following months, a more specific definition of an MIE emerges. ITAC produces a number of references to groups that encompass this definition. One note from November 2008 states they have 'included, among other things, opposition to US foreign policy, including the 'Global War on Terror', various Third World and regional causes, as well as animal rights, anti-globalization'. In some instances, the category MIE is directly associated with the global justice movement. An ITAC report from 22 September 2009, offers a clear example:

> There are cycles of protest and violence within this milieu, but common causes are opposition to perceived resource exploitation, infringement on aboriginal rights and cruelty to animals. A decade ago, activists within this milieu coalesced around mass protest, as in Quebec City in April 2001.

Within these broad categorical definitions of MIE, CSIS details a number of groups and events that are notable because of their connection to CSIS's understanding of 'sabotage' and their post-Cold War re-orientation. A report on 'the domestic terrorism situation' dated 30 August 2008 details a number of groups, including Al-Qaeda, Québec sovereigntists, 'lone wolf' attackers and cults. However, large portions of the report deals with left-wing activism, with such references such as: 'Extremists within the animal rights and environmental movements, [redacted] have a history of conducting attacks against facilities [redacted] in Canada'.

An underlying characteristic of these groups lumped in the category MIE – although often not stated – is their willingness to use publicity strategies and/or direct action tactics.[19] These range from media stunts, to blockades, to property destruction. The category of MIE thus blurs 'extremism' with public dissent. CSIS increasingly blurs categories of 'terrorism' and 'extremism', by which 'extremism' becomes a catch-all for a host of groups associated with civil disobedience and direct action. While not focused on mysterious clandestine groups, ITAC includes groups with high public profiles, including People for the Ethical Treatment of Animals (PETA) and, the most frequently cited group in all the Threat Assessments, Greenpeace.

ITAC reports lump together an exceptionally broad number of groups – no matter how distinct their tactics – into the aggregate category of MIE. Such groups are framed as threatening national security interests. An ITAC report prepared in November 2008, states that 'MIEs are non-hierarchical and amorphous in nature, and encourage members to form their own cells and carry out independent attacks'. The report, emphasising the domestic 'terror' threat of MIEs, warns:

> While Multi-issue extremist (MIE) attacks tend not to be spectacular mass-casualty attacks, a February 2008 study in the US concluded that MIE attacks are seven times more likely to occur than terrorist attacks. Therefore, due to the relative frequency of such attacks, MIEs actually cause more aggregate physical and financial damage than terrorists.

The blurring of terrorism/extremism is accompanied by a re-conceptualisation of what constitutes a threat to the Canadian public. Traditionally terrorism involves violence against civilian populations. Frequent mention of MIE 'attacks' by CSIS and the reference above to 'spectacular mass-casualty attacks' in the context of 'physical and financial damages' is misleading. CSIS presents MIEs as threats to public infrastructure and private property, and civilians as well. Yet no group mentioned within the MIE category have deliberately harmed or attacked a civilian populations.[20] Nonetheless, CSIS blurs the protection of private property – especially the property of Olympic corporate sponsors – within the rubric of national security. This deliberate classification slippage and the frequent mention of protests as forms of 'attacks' result in the following conclusions contained in a November 2008, ITAC report: 'AQ-inspired groups, MIEs, and aboriginal extremists have demonstrated both the intent and capability to target critical infrastructure in Canada, although no incidents involving these groups occurred during the reporting period'. The conceptualisation of national security threats morph in these reports where ITAC explicitly twins Al-Qaeda with domestic activism in a way that targets dissent. The MIEs and 'aboriginal extremists' referenced are accompanied by various examples of property destruction actions, such as broken windows, railway blockades, even boycott campaigns and other public education initiatives such as tabling sessions.

In addition to the blurring of terror/extremism, CSIS invokes the use of 'critical infrastructure' in their defence against sabotage. While early Threat Assessments discuss nuclear facilities and other sensitive *public* infrastructure such as electric power lines, ITAC reports indicate that MIEs are exclusively focussed on the disruption of *private* property, particularly the corporate sponsors of the Games. In one assessment, a reference to a Greenpeace media stunt near an Alberta oil sands development, ITAC warns: 'issue-based groups continue to use direct action tactics in protest against the operations of domestic and foreign energy companies'. This substantiates the point made by other authors (see Cowen and Bunce 2006, Collier and Lakoff 2008, Walby and Monaghan 2010) that security and intelligence agencies invoke the idea of 'critical infrastructure' as justification for reassignment of policing resources.

Indeed, as the Olympic Games approached, the idea of 'critical infrastructure' was expanded to include a diversity of objects. Gone from these reports are nuclear plants and power lines; in their place, corporate symbols are described as in need of protection. As an ITAC report prepared in April 2009 states, corporate symbols of the Games became a principle concern of for anti-terror policing:

> Games symbols have already been targeted, such as the Olympic clock, Olympic flag, corporate sponsors, like the Royal Bank of Canada and promotional events, for example, the recently concluded cross-Canada Olympic Spirit Train...in the form of protests, demonstrations, acts of vandalism, mischief, and threatening internet postings. Anti-Games actions have also included road, bridge and rail blockades, office occupations and arson. Calls have also been made for economic sabotage, mass convergence, airport, ferry, telecommunications and train disruptions, though these threats have not been acted upon.

While the Games approached, ITAC increasingly represented the corporate symbols of the Games as integral to the national interests of Canada. The blurred categories of activism, extremist, and terrorism, provide a presentation of 'facticity' (see Innes *et al.* 2005) where almost any expression of opposition is equated with the threat of violence against civilians. A November 2009, ITAC report states:

> Domestic extremists maintain the intent and capability to carry out attacks against property in Canada. Given the use of direct action tactics by domestic extremists, the threat of serious violence cannot be discounted.

As the Games approached, the abstract threat of Al-Qaeda, Hamas, and company had been overshadowed by a caricature of domestic protest activities, particularly direct action groups. The final ITAC report that we obtained, issued 19 January 2010, states: '[redacted]... the incidents and the threats against 2010 OPWG related events have emerged from the Multi-Issue Extremism (MIE) and the Aboriginal Extremism'. The threat of financial terrorism, which was the primary focus of the earliest reports, is not mentioned, nor does this report pay much attention to 'threats' other than grassroots political opposition.

The construction of the MIE terror identity emerges before the Games as the primary source of national security concern. Past studies on social movement repression (see Marx 1979, Boykoff 2007, Kinsman and Gentile, 2009) demonstrate how surveillance programmes target, then problematise and criminalise, social movements that present a challenge to the status quo. In the context of MIEs, however, there is a notable distinction that is unique to the contemporary state of politics under the Global War on Terror. The primary focus of this new security intelligence hub is the emergence of the global justice movement as a force confronting global capitalism. Perhaps most striking in these Threat Assessment reports is the absence of labour as a challenge to the status quo. Within the history of social movement repression in Canada, labour has historically figured as a target of police intervention. However, these ITAC reports indicate that threats from 'new new social movements' (Graeber 2002, 2010) – a combination of eco, indigenous and anarchist movements – have emerged as a preeminent concern for national security agencies.

The centralisation of intelligence has resulted in a new framework for anti-terror policing where subversive and simply suspicious conduct is lumped under the categories of terrorism and extremism. Gill (2006) refers to this as a weakening of due process in the field of security intelligence and criminal justice. To provide another example, we point to a category within Threat Assessment reports that first appeared in May 2005, under the heading 'Mentally Unstable Persons'. The section reads:

> Although mentally unstable individuals are cause for some concern, they are often just disruptive. However, it will be important to identify such individuals and to determine any propensity for violence among those identified.

In 2006 and 2007, the exact same text appeared under the heading 'emotionally disturbed persons'. In January 2008, however, a new heading titled 'Persons of Interest' (POIs) replaces the headings 'Mentally Unstable Persons' and 'emotionally disturbed persons'. The content of the section is subtly changed to:

> POIs are individuals that make direct or indirect threats against the Vancouver 2010 Games. Such persons may not pose a specific threat and are often merely disruptive; however it will be important to continue to identify them and to assess their propensity for violence.

In early 2008, POI sections of these reports begin to expand, and are mostly redacted under privacy exemptions. Appearing under sections of public order and domestic terrorism, we know through *Privacy Act* requests publicised after the Games that the POI category contains intelligence summaries on prominent activists. This shift from Mentally Unstable Persons to Persons of Interest offers further insight into how ITAC begins to re-frame domestic political opposition through the transformation of previously established and utilised categories.[21]

Discussion

In the foregoing analysis we have described the formation of intelligence clusters around recent mega-events in Canada. The ISU-JIG and the ITAC played a prominent role in creating and sharing intelligence reports. These reports were generated and shared across scales of policing, integrating local policing agencies into the national security intelligence network. Policing, security and intelligence agencies are thus networked through surveillance, in ways that extend capacities for suppression projects that aim to intimidate, harass and demobilise social movement groups. This coordination is not total, since the bureaucratic character of these agencies prevents full fusion (Deflem 2004). Although the ISU-JIG and ITAC are not organised with the intention of creating total information awareness as are similar agencies in the USA (see Monahan and Palmer 2009, Newkirk 2010), intelligence clusters in Canada provide an example of mission creep, where functions of these intelligence clusters extend beyond their original mandates, evinced in the shifting targets of 'financial terrorism' and Al-Qaeda to domestic political opposition, under the category of MIEs. We also demonstrate how these intelligence clusters engage in knowledge construction, creating 'terror identities' that become the rubric for further intelligence work. There is a tendency in intelligence work to rely on classifications, lumping all kinds of activities under umbrella terms as a way of making sense of them (Innes *et al.* 2005, de Lint 2008); the emergence of MIEs in Canada's federal security intelligence network provides a case in point.

The emergence of these intelligence clusters is directly related to the large-scale surveillance and security projects that accompany contentious mega-events. Boyle and Haggerty (2009) argue that these surveillance projects lead to the development and circulation of specialised security knowledges. We have emphasised how some of the classifications have been developed in the last half decade, especially as it concerns the ISU for the Vancouver Olympics. But we have placed less emphasis on the spectacle of security and more significance on how these efforts at securitisation lead to suppression of public opposition to mega-events when preconditions for dissident action are inhibited by 'either raising their costs or minimizing their benefits' (Boykoff 2007, p. 12). Surveillance also generates information that can lead to a transformation in how targets of suppression are categorised in intelligence reports.

Our analysis of the ISU-JIG and ITAC suggests that dissenting social movements have replaced so-called terrorism as the target of these intelligence clusters in Canada. Yet this has been accompanied by a shift in classification and the emergence of 'multi-issue extremism' as a special security knowledge. These classifications have created a novel 'organizing rubric' (Bowker and Star 1999, p. 3) for policing, security and intelligence agencies at the local and federal levels, blurring conventional scales of law enforcement and security.

Conclusion

Although largely focused Al-Qaeda and financial threats, the 2005 Preliminary Threat Assessment prepared by the RCMP's JIG contained a warning:

> As there will be extensive media coverage during the Games (20 billion viewers in 16 days), many protesters may view the Olympic Games as an ideal venue to confront the system of global corporate capitalism.

The ISU-JIG report is premised on the assumption that opposition to the Games would stem from ephemeral global movements. However, opposition to the Vancouver Olympic Games was rooted in local issues, led by indigenous land claims and anti-poverty struggles. Security agencies shifted their areas of concern as a result. Only when CSIS and the ITAC became the 'fusion centre' of Canada's intelligence community did the Threat Assessments begin to shift from abstract, distant terrorist threats towards tangible and imminent subjects of insecurity and dissent. This shift required the production of the MIE category of threat for the Canadian security establishment to re-imagine the threat posed by activists.

We have focused on transformations within knowledge networks (Brodeur and Dupont 2006) that connect policing, security and intelligence. Surveillance practices of Canada's national intelligence agencies shifted to explicitly target political opposition in the years leading up to three contentious mega-events. The blurring of threat categories has thus become a strategy of CSIS to rationalise domestic spying campaigns that target grassroots social movements. Our analysis has some consequence for understanding what is meant by 'surveillance' in the sociology of policing and security. Bell (2006, p. 157) argues that surveillance 'as a tool for classification is intended to detect, regulate and perhaps eliminate corrupting factors that threaten the security of the population'. This definition of surveillance explicitly focuses on the politics and consequences of surveillance. Likewise, our analysis lends itself to an understanding of surveillance that emphasises how intelligence gathering always takes place within a political context (see also Brodeur and Leman-Langlois 2006). In response to the perceived failures of security intelligence as it regards the events of 11 September 2001, 'doctrinal changes' (Gill 2004) or 'mission adaptation' (Deukmedjian and de Lint 2007) are altering the face of security intelligence in Canada. We have not focused on the up-take of new forms of national intelligence by municipal police. However, intelligence from the national scale is increasingly used at the local scale of policing (Gill 1998, Brodeur and Leman-Langlois 2006, Lippert and O'Connor 2006, de Lint and Hall 2009). Future research should explore how the 'terror identities' created by CSIS have become organising rubrics not only in federal-level agencies such as the RCMP and CSIS but municipal policing agencies.

Acknowledgement

We thank the *Policing & Society* reviewers D.T. Cochrane, S.P. Hier and J. Piché.

Notes

1. The Security and Prosperity Partnership, or SPP, was an attempt by the George W. Bush administration and leading North American corporations to connect the 'free trade' and anti-terror agendas. In August 2009, the SPP website stated it was no longer an 'active initiative'.
2. Due to this continuity, we often refer to the ISU as a single entity.
3. Despite the political importance of G8/G20 meetings of 2010, planning for the event was disorganised. Two related factors delayed the summit planning process: location selection and competing G8 and G20 agendas. The relative absence of the North American Leaders Summit (NALS) in the security assessments is due to the demise of the organisation. After its demise in 2007, the NALS was no longer mentioned in Threat Assessment reports. Over the course of 2005–2010, all the 'mega-events' were often mentioned in passing as part of a related security agenda, despite the overwhelming focus on the Olympic Games.
4. In an interview with senior military command Lieutenant-Colonel Pat Koch, the senior Canadian Forces (CF) planner in the ISU said: 'The Games have created an evolutionary change in the CF and RCMP in terms of how we work together. The results are permanent adaptations of collaborative and institutional policy and procedures that set the conditions for future domestic security events' (cited Thomas 2010).
5. This parallels what Diab (2008) calls a shift from evidence to intelligence within criminal trials in the post-11 September 2001 Canadian context.
6. The Vancouver ISU is officially known as the VISU and is, technically, separate from the G8/G20 ISU. However, we do not distinguish between these ISUs as their central elements – RCMP, CSIS, the Canadian army and several federal departments – remain consistent actors in both ISUs. The difference between VISU and G20ISU rests in different inclusion of local agencies. VISU included Vancouver and other proximate police services, while G20ISU included Toronto Police Services and the Ontario Provincial Police. Much of the information that proliferated between these hubs was aggregated by the ISU.

7. The final expenditure was over $900 million. Security costs for the G8/G20 in Toronto are expected to be over $1.2 billion. The Vancouver ISU started with a budget of $175 million.
8. This claim is based on reports in the *Vancouver Sun*, *Toronto Star*, and *Ottawa Citizen* concerning officers who had infiltrated social movement groups, sometimes for three years, leading up to the Olympic Games and G8/G20 meetings. In Vancouver, police posed as bus drivers, inviting activists into their bus apparently headed to Olympic Torch Relay disruptions.
9. The activist who undertook a national speaking tour critiquing the Olympics, mentioned above, was arrested *post-facto* in Vancouver under the charge of 'counselling mischief'.
10. All documents cited hereafter pertaining to CSIS were produced through ATIP request 117-2010-146. All documents cited hereafter pertaining to RCMP were produced through ATIP requests GA-3951-3-03551, GA-3951-00729, and GA-3951-A0174620. All our data can be accessed using these request numbers.
11. INSET was created after 11 September 2001 as an amalgamated anti-terrorism policing unit. Yet it has never assumed a position as an intelligence hub.
12. This list of acronyms partially substantiates our claim about 'mandate creep'. FAC stand for Firearms Academy Canada. TC refers to Transport Canada. CSC refers to Correctional Service of Canada, while CBSA refers to Canada Border Services Agency.
13. Although it is not clear from Nause's email, police agencies are responsible for Threat Assessment's pertaining to policing responsibilities other than national security issues during mega-events, including the guarding of Internationally Protected Persons.
14. Policy OPS-100 refers to part of the *CSIS Act* that sets protocol for targeting persons, groups, or events as security threats. It specifies how domestic and foreign agencies who work with CSIS must conduct intelligence investigations and reporting.
15. MIEs references do not exist before 2007, but Threat Assessments immediately begin re-creating their existence, *post-facto*. Reports frequently state that multi issue extremism began in the 1970s and 1980s, often mentioning the group Direct Action (Hanson 2001). A newsprint search reveals no mention of the term prior to 2009.
16. The use of the term 'militancy', as well as its subsequent transformation into 'extremism', reflects our claim about how security intelligence socially constructs threat categories.
17. The Sea Shepherd Conservation Society (SSCS) defends international environmental laws with the use of direct action tactics and media-oriented publicity campaigns.
18. The Yes Men are a satirical stunt group who impersonate individuals who are complicit in environmental and/or human rights abuses. Several stunts have targeted Canada's poor environmental record, including the launch of a mock Environment Canada website during a major international climate change conference in 2009.
19. Direct action movements are self-motivated by the ethics of participatory democracy and egalitarianism (Juris 2008, Graeber 2010). Some groups are strictly pacifistic, others advocate the use of self-defence only in the face of unmitigated violence.
20. Although they pre-date the existence of MIE as a category, Direct Action did inadvertently hurt a security guard in their bombing of an arms manufacturing facility in 1982 (Hansen 2001).
21. At other moments, ITAC reports blur their own categories in efforts to continuously conflate public expressions of opposition as potential acts of terror that imminently imperil national security. An April 2009 ITAC report illustrates: 'In Canada and abroad a change in protest tactics and tone of language appears to be occurring. Tactics against businesses seen to be exploitative have involved confrontational demonstrations, office occupations and low-level criminal damage. Social activist extremists now seem to be focusing on individuals rather than just corporations and their infrastructures. In conjunction with this, there has been an increased naming of public and private figures in numerous Internet postings which proclaim or call for violence. This can also be seen in the lyrics of some punk rocker bands'.

References

Bell, C., 2006. Surveillance strategies and populations at risk: biopolitical governance in Canada's National Security Policy. *Security Dialogue*, 37 (2), 147–165.

Berger, M. and Borer, D., 2007. The long war: insurgency, counterinsurgency and collapsing states. *Third World Quarterly*, 28 (2), 197–215.

Bigo, D., 2002. Security and immigration: towards a governmentality of unease. *Alternatives*, 27 (1), 63–92.

Bowker, G. and Star, S., 1999. *Sorting things out: classification and its consequences*. Cambridge, MA: MIT Press.

Boykoff, J., 2007. *Beyond bullets: the suppression of dissent in the United States*. Oakland: AK Press.

Boykoff, J., 2011. Space matters: the 2010 Winter Olympics and its discontents. *Human Geography*, 4 (2), 48–60.

Boyle, P. and Haggerty, K., 2009. Spectacular security: mega-events and the security complex. *International Political Sociology*, 3 (3), 257–274.

Brodeur, J. and Dupont, B., 2006. Knowledge workers or 'knowledge' workers? *Policing & Society*, 16 (1), 7–26.

Brodeur, J. and Leman-Langlois, S., 2006. Surveillance fiction or higher policing? *In*: K. Haggerty and R. Ericson, eds. *The new politics of visibility and surveillance*. Toronto: University of Toronto Press, 171–198.

Collier, S. and Lakoff, A., 2008. Distributed preparedness: the spatial logic of domestic security in the United States. *Environment and Planning D: Society and Space*, 26 (1), 7–28.

Cowen, D. and Susannah, B., 2006. Competitive cities and secure nations: conflict and convergence in urban waterfront agendas after 9/11. *International Journal of Urban and Regional Research*, 30 (2), 427–439.

Cunningham, D., 2004. *There's something happening here: the new left, the Klan, and FBI counterintelligence*. Berkeley: University of California Press.

Daase, C. and Kessler, O., 2007. Knowns and unknowns in the 'War on Terror': uncertainty and the political construction of danger. *Security Dialogue*, 38 (4), 411–434.

de Lint, W. 2008. Intelligent governmentality. *The Windsor Yearbook of Access to Justice*, 27 (2), 195–240.

de Lint, W. and Hall, A., 2009. *Intelligent control: developments in public order policing in Canada*. Toronto: University of Toronto Press.

Deflem, M., 2004. Social control and the policing of terrorism: foundations for a sociology of counter-terrorism. *The American Sociologist*, 35 (2), 75–92.

Deukmedjian, J. and de Lint, W., 2007. Community into intelligence: resolving information uptake in the RCMP. *Policing & Society*, 17 (3), 239–256.

Diab, R., 2008. *Guantanamo North: terrorism and the administration of justice in Canada*. Halifax and Winnipeg: Fernwood Publishing.

Dupont, B., 2004. Security in the age of networks. *Policing & Society*, 14 (1), 76–91.

Earl, J., 2009. Information access and protest policing post-9/11: studying the policing of the 2004 republican national convention. *American Behavioral Scientist*, 53 (1), 44–60.

Fernandez, L., 2008. *Policing dissent: social control and the anti-globalization movement*. Chapel Hill: Rutgers University Press.

Gill, P., 1998. Police intelligence processes: a study of criminal intelligence units in Canada. *Policing & Society*, 8 (4), 339–365.

Gill, P., 2004. Securing the globe: intelligence and the post-9/11 shift from 'Liddism' to 'Drainism'. *Intelligence and National Security*, 19 (3), 467–489.

Gill, P., 2006. Not just joining the dots but crossing the borders and bridging the voids: constructing security networks after 1 September 2001. *Policing & Society*, 16 (1), 27–49.

Graeber, D., 2002. The New Anarchists. *New Left Review*, 13, 61–73.

Graeber, D., 2010. *Direct action: an ethnography*. Oakland: AK Press.

Hansen, A., 2001. *Direct action: memoirs of an urban guerrilla*. Toronto: Between the Lines.

Innes, M., Fielding, N., and Cope, N., 2005. Appliance of science? The theory and practice of crime intelligence analysis. *British Journal of Criminology*, 45 (1), 39–57.

Jensen, K., 2009. *Cautious beginnings: Canadian foreign intelligence 1939–51*. Vancouver: University of British Columbia Press.

Juris, J., 2008. *Networking futures: the movement against corporate globalization*. Durham, NC: Duke University Press.

Kinsman, G. and Gentile, P., 2009. *The Canadian war on queers: national security as sexual regulation*. Vancouver: University of British Columbia Press.

Larsen, M. and Piché, J., 2009. Exceptional state, pragmatic bureaucracy, and indefinite detention: the case of the Kingston immigration holding centre. *Canadian Journal of Law and Society*, 24 (2), 203–229.

Lippert, R. and O'Connor, D., 2006. Security intelligence networks and the transformation of private security. *Policing & Society*, 16 (1), 49–65.

Manning, P., 2006. Two case studies of American anti-terrorism. *In*: J. Wood and B. Dupont, eds. *Democracy, society and the governance of security.* Cambridge: Cambridge University Press, 52–85.

Marx, G., 1979. External efforts to damage or facilitate social movements: some patterns, explanations, outcomes and complications. *In*: M. Zald and J. McCarthy, eds. *The dynamics of social movements.* Minnesota: Winthrop Publishers, 94–125.

Marx, G., 1984. Notes on the discovery, collection, and assessment of hidden and dirty data. *In*: J. Schneider and J. Kitsuse, eds. *Studies in the sociology of social problems.* Norwood, NJ: Ablex, 78–113.

Monahan, T. and Palmer, N., 2009. The emerging politics of DHS fusion centers. *Security Dialogue*, 40 (6), 617–636.

Neocleous, M., 2008. *Critique of security.* Edinburgh: Edinburgh University Press.

Newkirk, A., 2010. The rise of the fusion-intelligence complex: a critique of political surveillance after 9/11. *Surveillance & Society*, 8 (1), 43–60.

O'Bonsawin, C., 2010. 'No Olympics on stolen native land': contesting Olympic narratives and asserting indigenous rights within the discourse of the 2010 Vancouver games. *Sport in Society*, 13 (1), 143–156.

Piché, J. and Walby, K., 2010. Problematizing Carceral Tours. *British Journal of Criminology*, 50 (3), 570–581.

Roberts, A., 2006. *Blacked out: government secrecy in the information age.* Cambridge: Cambridge University Press.

Roche, M., 2000. *Mega-events and modernity: Olympics and expos in the growth of global culture.* London and New York: Routledge.

Sethna, C. and Hewitt, S., 2009. Clandestine operations: the Vancouver women's caucus, the abortion caravan, and the RCMP. *The Canadian Historical Review*, 90 (3), 463–496.

Shaw, C., 2008. *Five ring circus: myths and realities of the Olympic games.* Gabriola Island, BC: New Society Publishers.

Sheptycki, J., 1998. Policing, postmodernism and transnationalization. *British Journal of Criminology*, 38 (3), 485–503.

Thomas, D., 2010. Inside Olympic security. *The Maple Leaf*, 13 (2), 20.

Tsoukala, A., 2006. The security issue at the 2004 Olympics. *European Journal for Sports and Society*, 3 (1), 43–54.

Voulgarakis, G., 2005. Securing the Olympic Games: a model of international cooperation to confront new threats. *Mediterranean Quarterly*, 16 (4), 1–7.

Walby, K., 2009. 'He asked me if I was looking for fags...' Ottawa's national capital commission conservation officers and the policing of public park sex. *Surveillance & Society*, 6 (4), 367–379.

Walby, K. and Larsen, M., forthcoming. Getting at the live archive: on access to information as data collection in Canada. *Canadian Journal of Law and Society.*

Walby, K. and Lippert, R., forthcoming. Spatial regulation, conservation officers, and dispersal policing of homeless people in Ottawa, Canada. *Antipode.*

Walby, K. and Monaghan, J., 2010. Policing proliferation: on the militarization of police and atomic energy Canada Limited's nuclear response forces. *Canadian Journal of Criminology and Criminal Justice*, 52 (2), 117–145.

Walby, K. and Monaghan, J., 2011. Private eyes and public order: policing and surveillance in the suppression of animal rights activists in Canada. *Social Movement Studies*, 10 (1), 21–37.

Copyright of Policing & Society is the property of Routledge and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.