Routledge
Taylor & Francis Group

Contemporary Justice Review
Issues in Criminal, Social, and Restorative Justice

ISSN: 1028-2580 (Print) 1477-2248 (Online) Journal homepage: https://www.tandfonline.com/loi/gcjr20

Surveillance of environmental movements in Canada: critical infrastructure protection and the petro-security apparatus

Jeffrey Monaghan & Kevin Walby

To cite this article: Jeffrey Monaghan & Kevin Walby (2017) Surveillance of environmental movements in Canada: critical infrastructure protection and the petro-security apparatus, Contemporary Justice Review, 20:1, 51-70, DOI: 10.1080/10282580.2016.1262770

To link to this article: https://doi.org/10.1080/10282580.2016.1262770

CONTEMPORARY JUSTICE REVIEW, 2017
VOL. 20, NO. 1, 51–70
http://dx.doi.org/10.1080/10282580.2016.1262770

Routledge
Taylor & Francis Group

Surveillance of environmental movements in Canada: critical infrastructure protection and the petro-security apparatus

Jeffrey Monaghan[a] and Kevin Walby[b]

[a]Institute of Criminology and Criminal Justice, Carleton University, Ottawa, Canada; [b]Department of Criminal Justice, University of Winnipeg, Winnipeg, Canada

ABSTRACT

A convergence of post-9/11 security governance practices and a dependence on extractive economies has resulted in changes to the way Canadian policing agencies classify environmental movements. We detail how the category of 'critical infrastructure protection' (CIP) now enables surveillance of environmentalists under the banner of national security. We examine the growth of CIP as a security category, its changing character from the Cold War to the present, and the role of threat entrepreneurs. We demonstrate that CIP networks have institutionalized collaborations between national security agencies and energy corporations, creating a petro-security apparatus that aims to suppress dissent. We conclude with reflections on what surveillance regimes driven by the petro-security apparatus mean for debates about national security and social movements.

ARTICLE HISTORY
Received 10 April 2015
Accepted 19 April 2016

KEYWORDS
Security; surveillance; social movements; critical infrastructure; policing

Introduction

As in other Western countries where surveillance targets social movements that threaten entrenched economic interests – particularly the United States (Amster, 2006; Ellefsen, 2012; Fernandez, 2008; Gillham, Edwards, & Noakes, 2013; Lubbers, 2012; Potter, 2011) – security agencies in Canada now classify environmental activities as domestic terrorist threats. The categorization of the environmental movement as a threat has mobilized substantial national security resources that facilitate monitoring sources of eco-unease. Despite the environmental movement's strong and long-standing affinity to non-violent protest, security agencies now regularly define the Canadian environmentalists as a potential source of violence.

The purpose of this article was to explain how the environmental movement has been constructed as a national security threat in Canada. To do so, we examine the transformation of 'critical infrastructure protection' or CIP as a discourse that enables domestic surveillance. Drawing from scholars who have examined CIP as a catalyst for national security initiatives (Aradau, 2010; Collier & Lakoff, 2008; Deibert & Rohozinski, 2010; Dunn Cavelty & Suter, 2008), we underline its significance for the targeting of social movements today. Though it derives from a Cold War era category focused on potential sabotage and espionage by state-based

CONTACT Jeffrey Monaghan jeffrey.monaghan@carleton.ca

actors, the security governance of CIP has undergone a recent transformation and expansion to become a heterogeneous field of menace that can include areas of traditional state-based espionage and sabotage; non-state threats associated with terrorism; as well as disruptions presented by social movements, computer viruses, traffic jams, and migratory birds. A substantive element of the CIP surveillance agenda is focused on imagined threats of the environmental movement. Further, we underline how CIP is a category impelled by the interests of energy sector corporations.

A number of scholars have pointed to trends in what O'Reilly (2010) calls security related 'state-corporate symbiosis,' examining how policing and corporate interests converge when they supply information and resources to one another (see also Crosby & Monaghan, 2016; Dorn & Levi, 2009; Lubbers, 2012; Walby & Monaghan, 2011). We suggest that CIP security practices are illustrative of the webs of cooperation between public police and major corporations that result in a distinct preferentialism toward private economic interests (Godfrey, Brewis, Grady, & Grocott, 2014; O'Reilly, 2010). Given that energy infrastructure governed by the CIP agenda is itself almost exclusively owned by large energy corporations, the relationships established under CIP exemplify a blending of the energy economy with the national security infrastructure of public policing agencies. As a contribution to research from the sociology of surveillance, our article suggests that public–private relationships fused through CIP security governance do not necessarily correspond with the criminal or terrorist worlds they claim to be reacting against, but instead should be understood as neo-liberal governance practices that rationalize the exclusion and surveillance of actors that are deemed as outsiders, critics, or hostile to economic development (Bajc, 2007). Labels can determine the exclusion of social actors and, for social movements categorized as threats, result in surveillance efforts aimed at suppression (Boykoff, 2007; Kinsman & Gentile, 2010). As an empirical domain to explore national security policing, we examine the CIP relationships established between national security agencies in Canada and what they refer to as 'their security peers' in major energy corporations. Underlying the peer-to-peer relations established between insiders of CIP security governance, we focus on how environmental groups have been produced as criminal outsiders by detailing the policing reaction to contentious protests over the proposed Enbridge Gateway pipeline.

Gateway is a contentious project that aims to move oil from the tar sands in northern Alberta to a terminal in Kitimat nestled along British Columbia's pristine coastal environment. A combination of the precarious pipeline route, the weighty ecological footprint of the tar sands energy production, and Canada's poor record on addressing climate change, has meant that environmentalists focused significant campaigning effort against the Gateway pipeline (McDiarmid, 2014). Our focus on the policing reaction to the environmental movement provides an account of how an assemblage of public and private entities coordinates their surveillance practices. We demonstrate how the surveillance web involves the national police force (RCMP), national intelligence agency (CSIS), independent pipeline review agency (National Energy Board (NEB)), a number of energy corporations (in particular the Enbridge Corporation), as well as private security firms. Surveillance includes open-source and covert methods, as well as widespread sharing of personal information between agencies. Though Canada lacks fusion centers organized in the US by the Department of Homeland Security (see Monahan & Palmer, 2009), we draw attention to similar intelligence practices have emerged in Canada under the rubric of CIP. In our examination of the state–corporate symbiosis, we point to recent efforts to coordinate surveillance through institutionalized

meetings between Enbridge and a network of Canadian security agencies. In preparing for contentious public pipeline meetings on the Gateway pipeline, where any critics of the pipeline project – whom are attempting to make public representations at the NEB – these meetings have become central in the typecasting environmentalists as violent social actors and thus as deviant 'outsiders.' The fusion of Enbridge and Canada's security apparatus is a conjoining of police and corporate power, which is demonstrative of the petro-security apparatus now institutionalized in Canada.

First we consider existing literature on CIP and surveillance. After a note on method, the second component of the article is divided among subsections that examine the surveillance of environmentalists opposed to the contentious Northern Gateway pipeline proposal. We investigate the emergence of RCMP Critical Infrastructure Intelligence Team (CIIT) threat assessments and suspicious incident reporting (SIR). We then examine the surveillance work of the RCMP CIP teams in relation to community hearings involving the Gateway pipeline. We look at how the CIIT maintained efforts at 'situational awareness' involving widespread surveillance of environmentalists for 'suspicious activity, criminal extremism, or other activities which could pose a threat to Canada's national security' (RCMP, 2013–5745, p. 125). While many of these groups – Greenpeace, Leadnow, ForestEthics Advocacy, the Council of Canadians, the Dogwood Initiative, EcoSociety, and the Sierra Club of British Columbia – attempted to be involved in the pipeline hearing process held by the NEB, state agencies characterized these groups as extremist threats. We use the notion of 'threat entrepreneurs' (Mueller, 2006) to conceptualize the role of security personnel who direct surveillance practices in these networks, and we demonstrate how threat entrepreneurs from public policing agencies have utilized the threat of social movements to formalize regular intelligence meetings between security agencies and energy companies on issues of CIP. Finally, we reflect on what surveillance regimes driven by the petro-security apparatus mean for debates about national security and social movements.

Making sense of critical infrastructure and surveillance

Critical infrastructure is an elastic notion that can be applied to any person, place, or thing that a state agency or corporation designates as significant (Lipschutz, 2008). An array of agencies engages in surveillance practices for the purposes of CIP. Palmer and Whelan (2006) have shown that CIP now involves numerous private agencies due to private ownership and operation of critical infrastructure but also private security intelligence agencies.[1] Pynnöniemi and Busygina (2013) argue old visions of totalizing state power do not work for understanding CIP, the latter of which is based on flexible strategies that prioritize public–private partnerships.

Much of the literature on CIP is practitioner oriented (Coward, 2009; Koski, 2011; Newbold & Delp, 2011; Quigley, 2013), which we consider shortsighted for three distinct reasons. First, practitioner literature accepts the classifications of threat that security intelligence agencies devise, which is faulty since these often conflate protest with extremism and criminality. Second, it accepts that security intelligence and national security surveillance practices provide public safety when, as we show below, these practice tend to narrowly represent the interests of industry and energy companies. Third, practitioner literature fails to raise questions about authority, power, and how security intelligence and surveillance exacerbate such social problems.

Because most critical infrastructure is owned and operated by private corporations, the effort to govern CIP-related security threats has produced a web of police and corporate relations. An illustration of the fusion of state and corporate agendas in the field of CIP is exemplified by ASIS International seminars on CIP for its members.[2] In Canada, there have been a number of formalized means to intake security and surveillance data from private companies, some of which we address below. However, we underline that state security agencies are central hubs in what Brodeur has conceptualized as a policing assemblage (Brodeur, 2010). National-level security agencies play a key role in organizing CIP-oriented surveillance, by coordinating hubs that draw specialists from multiple agencies who collaborate with provincial and local police as well as industry representatives. Special branches have emerged in Public Safety Canada and the RCMP such as the Critical Infrastructure and Strategic Coordination Directorate[3] of Public Safety Canada, and the RCMP's Critical Infrastructure Suspicious Incident Reporting unit.

Bajc's (2007, p. 1651) work on security meta-rituals is illustrative for conceptualizing national security and surveillance in this case. She argues that national security practices of surveillance are ritualistic. Part of the ritual is deciding who is an insider and who is an outsider (to be targeted by surveillance). What she calls a 'security meta-ritual' refers to repeated acts of surveillance coordinated by state agencies that target outsiders and block their access to social spaces or events deemed to be of special significance. In the context of critical infrastructure, those who are disapproving of pipelines must be constructed as outsiders and kept away from this infrastructure. Construing activists as outsiders justifies the ritual in a self-fulfilling manner, which not only bars dissenters from nearing the sites they are critical of, but further functions to exclude their criticisms from public debates about critical infrastructure development, particularly on expansion of the tar sands.

CIP in Canada

CIP has its roots in Cold War policies (Collier & Lakoff, 2008). Much of the focus during the Cold War was targeting suspected communist functionaries (Kinsman, Buse, & Steedman, 2000; Whitaker & Marcuse, 1994), and the threat of sabotage or industrial espionage was secondary. Cold War strategies on critical infrastructure are only an aspect of the larger security state structured by the ideological battles of the bi-polar world. As Bigo (2006), p. 393 notes, with the end of the Cold War, Western states have reorganized the categories used to analyze security 'since the matrix has rotated,' and invented new ways to describe threats using 'an unchanged grammar with a new vocabulary.' In Canada, discourses of industrial sabotage have been replaced with a diverse vocabulary reflecting targets of today's security apparatus.

This shift in security discourse has created an expanded articulation of critical infrastructure. A CSIS memo written in 2008 details, when the *CSIS Act* was written in 1984, 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' (CSIS, 2009-143, p. NP). The memo notes that 'sabotage has been a favourite tool used by environmental and biocentric militants and extremists to further their ideological or political agenda.' Citing examples of tactics that 'cause economic damage to private enterprises' like tree-spiking, sabotage of logging machinery, alleged food contamination, CSIS warns that the threat extends 'to more serious acts that target critical infrastructure and function as so-called force multipliers'

(*ibid*.). With a post-Cold War threat environment extending beyond the acts of foreign governments, CIP rationalizes a more active Canadian security establishment.

CIP has been a growing component of the reorganization of security governance post-9/11.[4] Canada released its first national security strategy in 2004 (Canada, 2004a). The *Strategy* pledged to release a full position paper on CIP after consulting with the private sector and the United States 'to drive forward a national process that prioritizes substantial improvement of our national capabilities in critical infrastructure protection' (Canada, 2004a, p. 26). Published by the Department of Public Safety and Emergency Preparedness in November 2004, the position paper (Canada, 2004b, p. 5) provides a broad definition. Fusing natural disasters with terrorism events and cyber-security, CIP is defined as consisting of those 'physical and information technology facilities, networks, services and assets, which if disrupted or destroyed would have a serious impact on the health, safety, security or economic well-being of Canadians or the effective functioning of governments in Canada.' With the ownership of CIP in the hands of major corporations, the policy paper relies on the pledge to conduct 'stakeholder' consultations. A final recommendation was to release a comprehensive National Critical Infrastructure Protection Strategy. Although it was significantly delayed, the *National Strategy for Critical Infrastructure* (Canada, 2009a) was released in parallel with *Action Plan for Critical Infrastructure* (Canada, 2009b) in 2009. Canada's CIP strategies (Canada, 2009a, 2009b) identify 10 separate economic sectors that fall within critical infrastructure and underlines an 'all hazards approach' that includes natural disasters and terrorism. Given its delay, the CIP *National Strategy* and *Action Plan* are small publications, short on detail, and consisting mostly of claims about resiliency (Coaffee, Murakami-Wood, & Rogers, 2008; Lentzos & Rose, 2009) around its 'three elements' of partnerships, risk management, and information sharing. The core legacy of the CIP strategy is the prioritization of critical infrastructure at the center of the national lexicon for discussing threat preparedness.

The CIP policing assemblage is steered at the federal level but extends to all regions and involves cross-border coordination. For instance, in a 12 November 2009 presentation by Acting Regional Director, Ontario, Public Safety Canada, as well as Critical Infrastructure Coordinator, Ontario, Public Safety Canada, for the 2010 G8 Joint Intelligence Group Workshop, it is noted that 'The committees comprise federal, state, local and private authorities to enhance security efforts along the Canada-US border in the Great Lakes area' (PSC 2009-00280, p. 22). The policing assemblage engenders a proliferation of working groups, secretariats, and forums addressing CIP issues. Yet, at the federal level, CIP issues are addressed by few departments, primarily Transport Canada, National Resources, and the security establishment (RCMP, Public Safety, and CSIS). In practice, CIP issues are managed by agencies focused on terrorism, which has resulted in a prioritization of 'human induced' events at the expense of weather related or 'natural' events. With a focus on human induced events (such as protests), CIP security governance has centered a need to protect the energy industry from threats like the environmental movement.

In rationalizing these surveillance practices, security agencies make reference to the 'extremist' elements of the environmental movement who engage in violence. While examples of criminalization and harassment exist in the early period of the environmental movement, it was not until the 1990s that discourses of 'terrorism' and 'extremism' became popular frames for categorizing eco-activists. The case of Wiebo Ludwig is the most notable example of security agencies using the lexicon of 'eco terrorism' (Nikiforuk, 2001). During the RCMP's

Operation Kabriole in Alberta, the policing service used a number of dirty tricks, including a withdrawn proposal to car bomb a company vehicle, as well as a carrying through with a staged explosion of a remote gas well to build a media panic around eco-terrorism. Relying on informant-produced evidence, Ludwig was convicted of using explosives to sabotage oil and gas wells. Ludwig's case remains a reference point for security agencies in Canada.

Though Canada's environmental movement has no history of violence toward civilian populations and only a sprinkling of anecdotes related to significant property destruction, security agencies have employed broad language of 'extremism' and focused on business disruptions and property damage as national security threats. To demonstrate how security bureaucracies ritualize the identities of eco-actors as extremist threats, below we focus on surveillance of those opposed to the Gateway Pipeline proposal.

Design and methods

As part of a broader, continuing research project on security intelligence practices and political policing in Canada, we used access to information (ATI) to locate threat assessments, emails, PowerPoint presentations, and other internal documents within RCMP, Public Safety Canada, Transportation Canada, Canada Border Services Agency, and CSIS. As a module in our regular submission of ATI requests at the federal level to several agencies involved in policing and intelligence, we received approximately 1900 pages of material on CIP-inspired surveillance. We focus on activities between 2009 and 2014, although much of our analysis focuses on 2011–2012 as the most concentrated period of surveillance. We coded this material for mentions of CIP, excerpts on how CIP is carried out, excerpts on who or what is construed as a threat, excerpts on specific movements or groups, as well as mentions of any documents, presentations, emails related to CIP that we could locate with subsequent ATI requests. These data were coded for events and practices related to surveillance, and for discourses that frame activists as threats. These data examined here are representatives of our sample of 1900 pages, which are explanatory (Stake, 1995) since they express the general tendency with the practices being examined. Certainly, discussing contemporary practices of national security can engender roadblocks in the production of research data. As one sheet from the records we discuss notes succinctly: 'Please do not share this document outside law enforcement and CSIS' (RCMP, 2013-05745, p. 110). Despite barriers, when internal records are released, they can allow us to explore how the regularized surveillance of eco groups is premised on the characterization of their intentions as potentially violent.[5]

Analysis

CIIT threat assessments and suspicious incident reporting

To provide context for understanding the policing assemblage created to facilitate CIP in Canada, next we explain the role of RCMP Critical Infrastructure Intelligence Team (CIIT) threat assessments, and suspicious incident reporting. The CIIT inspects 'physical and cyber threats to critical infrastructure in support of the RCMP's and Government of Canada's critical infrastructure protection mandates' (RCMP, 2013-013180, p. 2). As a central node of the assemblage, the CIIT operates in collaboration with domestic partners, including 'Public Safety Canada, CSIS, and the Integrated Terrorism Assessment Centre (ITAC); provincial

government agencies; private sector stakeholders; and international partners such as security and police partners in the United States, United Kingdom and Australia…' (*ibid*.).

CIIT threat assessments are condensed results of intelligence gathering and incident reporting. As documents that aggregate a litany of potential national security threats, the assessments are shared to provide stakeholders with law enforcement intelligence assessment of CIP issues, and have investigated many issues construed as threats to critical infrastructure. For instance, on 16 September 2011, Timothy O'Neil (Senior Criminal Intelligence Research Specialist, CIIT) sends an email regarding a CIIT assessment referring to the anti-Keystone pipeline protests in Ottawa. He notes that 'both open source background information and law enforcement intelligence have indicated that persons opposed to Canada's petroleum industry have expressed intent and demonstrated capability to engage in non-violent criminal activity against Canada's energy sector' (RCMP, 2012-02817, p. 1). The document goes on to suggest that 'It is highly likely that protest actions on 2011-09-26, will include acts of unlawful civil disobedience that will result in arrests…protest actions may be conducted elsewhere in Canada, targeting Oil Sands and other petroleum facilities and financial institutions associated to the petroleum industry… Environmental activists' actions may inadvertently result in personal injury/death, damage to facility's infrastructure and to the natural environment' (RCMP, 2012-02817, p. 5). Stakeholders are asked to report suspicious activity to local law enforcement, the National Security Information Network, as well as CSIS.

Throughout these documents protestors are described as violent and extremists, and several eco groups are listed as suspicious and targeted with surveillance because of supposed 'non-violent criminal activity' (RCMP, 2012-02817, p. 1). Though security agencies such as the RCMP and CSIS have never revealed any protocols that guide their classification regimes, we note that 'non-violent criminal activity' and 'violence' are the two primary discursive labels attached to eco groups. The use of these labels by RCMP and CSIS overlap is used interchangeably, as well as simultaneously – especially in reference to groups like Greenpeace.

A review of the CIIT's inconsistencies on the assessment of violence further illuminates conflation of social movements with terrorism. Although much of the Canadian security establishment's attention is directed toward potential Islamic threats the categories of CIP regularly allow for environmental activists like Greenpeace to be included in conjunction with threats from Al-Qaeda or others with the explicit aim of harming civilian populations. In one 2011 document, the CIIT detailed several 'potential threats to critical infrastructure (CI)' (RCMP, 2013-013180, p. 7). It begins with an Islamist plot to suicide bomb the New York subway system. The threat assessment then shifts to the potential threat of cyber-attacks targeting Finance Canada and the Treasury Board of Canada Secretariat (on cyber-security and CIP, see Deibert & Rohozinski, 2010). The document then shifts to domestic concerns of a different type, suggesting that there are an increasing number of anti-fracking incidents within Canada in Quebec and New Brunswick, where hundreds of public demonstrations had resulted in heated public debates on shale gas extraction. Notably, the threat assessments are produced at the same time as the RCMP was engaged in covert efforts to disrupt environmental movements in New Brunswick (Howe, 2015). Notwithstanding, the CIP threat assessments highlight that anti-fracking actions in New Brunswick resulted in roughly $250 000 and included allegations of threatening letters and phone messages against companies involved in the shale gas industry. An investigation resulted in a male being arrested and charged with 12 criminal code offences, including anti-terrorism charges. As a CIIT threat

assessment concludes, given 'the increasing number of criminal incidents and *the level of violence* targeting the Canadian shale gas industry, there is also the very real possibility that Canadian anti-fracking activists may link up with their U.S. counterparts to compare and develop protest/direct action techniques' (RCMP, 2013-013180, p. 26, emphasis added). After the summaries of threats from Al-Qaeda to shale gas activism, the reader is left with an implicit equivalence between threatening phone calls, vandalism, and blowing up strangers on a packed subway system. As a process of aggregating threats in the defense of CIP, this type of threat construction displays the lack of categorical certainty that accompanies a concept as central to order maintenance as violence. Conflations of crime, violence, and protest with other terrorism threats are an aspect of the petro-security ritual that justifies the designation of eco-protests as deserving routine surveillance from national security agencies.

Another RCMP CIIT assessment dated 26 September 2011 on the Anti-Keystone Pipeline Ottawa Protests presents similar conflations of protests and violence. The assessment notes that in an effort to mirror the Washington D.C. anti-Keystone protests an open invitation to engage in symbolic civil disobedience – i.e. crossing a police line and receiving a fine – was posted on the website of a civil society group called the Council of Canadians. Suggesting a link to potential national security issues, the RCMP threat assessment reports that Greenpeace Canada, the Council of Canadians and the Indigenous Environmental Network, '…are asking you to come to Ottawa (on 2011-09-26) to participate in one of the largest acts of civil disobedience on the climate issue that Canada has even seen…stand up to Prime Minister Harper [and] the tar sands industry' (RCMP, 2012-02817, p. 4). The assessment also notes that there has been increased opposition to the petroleum industry including a rise in 'criminal activity' beyond Alberta, citing the anti-shale gas protests in New Brunswick. The CIIT noted unconfirmed reports that 'extremists' (including those associated with the Occupy movement) could be planning on using smart mob tactics to disrupt traffic and business operations. The actions of the smart mob 'could result in the denial of the legal access to buildings and roadways and may jeopardize the personal safety of company employees and the general public if the mob prevents law enforcement and other first responders from responding to a particular incident' (RCMP, 2013-013180, p. 30). Through the extrapolation of potential harms, the RCMP suggests that these protests require enhanced surveillance focused on Greenpeace, the Indigenous Environmental Network, and the Council of Canadians. These are just a few examples of CIIT threat reporting that construe protestors as national security threats. Such surveillance is used to sort some people out as not belonging, and Canadian security agencies have a record of targeting groups that deviate from the norm as threats to society (Kinsman & Gentile, 2010). As Bajc (2013, p. 3) argues, 'classifications for the purposes of surveillance…are exclusionary…such taxonomies are purposefully invented by various officials and operatives with the goal to control social behavior and social change through the means of surveillance.' CIP categories conflate a spectrum of public opposition as forms of criminal security threat, rationalizing efforts targeting environmental movements.

CIIT threat assessments are compiled in part by synthesizing open source and covert intelligence as well as results of Suspicious Incident Reporting (SIR) from sources such as the Critical Infrastructure Suspicious Incident Reporting program within the RCMP. SIR enrolls agencies and agents (including corporate agents) to report any suspicious activities to the RCMP who would then react against any supposed threats. In 2008, the CIIT launched the

pilot project for use in the Rail and Urban Transit sector, and was later expanded to include more stakeholders. In June 2010, the SIR system went online and was made available to all stakeholders in Transportation, Energy, and Finance. In this way, CIP engenders new forms of national security reporting and public vigilance (Pynnöniemi & Busygina, 2013).

In one bi-annual CIIT-SIR assessment, the CIIT section thanks all stakeholders as well as property management groups who have contributed to the SIR system, including other national security agencies and local stakeholders and law enforcement agencies. The CIIT finally thanks Transport Canada, Natural Resources Canada, Finance Canada, and the Bank of Canada stakeholders and government sector leads as they expand the SIR system (RCMP, 2011-016328). This list demonstrates the scope of the policing assemblage created to facilitate CIP, and the number of players inside and outside the conventional security intelligence domain who are drawn together under the category of CIP threats.

CIP surveillance and the gateway pipeline

In December 2009, Enbridge put forward an application to the NEB for an environmental review of the project – a first step in obtaining project approval from federal regulators. Enbridge's proposal to build the Gateway pipeline solicited immediate opposition from a broad spectrum of civil society, environmental and indigenous groups. Given the history of land theft in British Columbia (see Harris, 2004), the notion that Enbridge would build the pipeline through unceded territory resulted in a number of contentious demonstrations and threats of legal action (Kulchyski, 2013; McCreary & Milligan, 2014). Over 100 indigenous groups have signed declarations against the pipeline and, given the precarious route through unceded territory and pristine wilderness, over 26,000 settler allies have pledged solidarity with indigenous campaigns to 'hold the wall.'[6] Combined with the perceptions that the pipeline negotiations were taking place in secrecy, Gateway became symbolic of a number of environmental and social justice issues that accelerated protests and critical public attention.

While the first panel was held in January 2012, the RCMP began security preparations after Enbridge had submitted their proposal in late 2009. The RCMP's National Security Criminal Intelligence (NSCI) unit hosted a working group meeting on 8 August 2010 at RCMP Headquarters in Ottawa. Titled the 'Enbridge Northern Gateway Pipeline Project- Intelligence Production Meeting,' the RCMP CIIT held the session 'to discuss the intelligence production requirements as they pertain to the planning and development of the Enbridge Northern Gateway Pipeline' (RCMP, 2013-05745, p. 229). Attendees included CSIS, RCMP Criminal Intelligence, RCMP E and K Divisions, and Enbridge.

In summarizing intelligence products for the consultation process, the invitation for the meeting warns that 'a variety of national and international groups, some of which may ultimately resort to criminal actions to prevent or interfere with the building of the Project' (RCMP, 2013-05745, p. 233). The objective was to provide 'a forum to discuss security concerns relating to the pipeline project, with the objective of developing an integrated intelligence production plan' for distribution among security actors involved with surveillance of eco actors. Meeting summary notes outline a 'discussion' where participants praise the economic benefits and safety of the pipeline. In highlighting that 'the financial benefits of the pipeline to the Canadian (including the Alberta and B.C.) economy are well documented, as are the benefits to the U.S. and possibly Asian energy markets,' the notes emphasize that the

'construction, operation and maintenance' will adhere with 'strictly enforced federal government regulations which will include consideration for the health and safety of Canadians, Aboriginal concerns, and the safety of the natural environment' (RCMP, 2013-05745, p. 179). Further, the RCMP notes 'there is wide support for the building of the pipeline' from trade unions, pipe providing companies, support/services industries. The RCMP suggests that 'there be many spin-off jobs created during the construction of the pipeline, and there will be legacy jobs created to maintain the pipeline during its lifetime' (RCMP, 2013-05745, p. 179). In concluding, the RCMP advices that 'those opposed to the pipeline project include some associated to: Aboriginal sovereignty concerns; a variety of environmental awareness groups; and others who may be impacted during the construction and the subsequent life of the pipeline.' These three categories of opponent supply a caricature of anti-social deviants: upset First Nations, unreasonable environmentalists, and complainers. This creation of castigated outsiders is germane to state surveillance (Bajc, 2007). Project opponents are caste out of the arena of respectable 'stakeholders,' leaving only the corporations as 'insiders' in the NEB hearings.

An outcome of the meeting was that the RCMP pledged to 'collaborate in the production of associated classified and unclassified intelligence products' with 'other law-enforcement agencies, other federal and provincial departments; related stakeholders and, not exclusively: [redacted]' (RCMP, 2013-05745, p. 179). The document emphasizes the role of integrating private intelligence when it notes that 'as, and if, required other stakeholders will be solicited for assistance in the production of the intelligence products' (RCMP, 2013-05745, p. 180). Within the RCMP, congratulations were passed to Senior Criminal Intelligence Research Specialist Timothy O'Neil for bringing Enbridge and private sector into the intelligence production circle. Wendy Nicol, from the NSCI Critical Infrastructure and Operational Assessment branch, sent an August 9th email to O'Neil. It reads: 'In the Officer's meeting Friday Larry mentioned your Northern Gateway initiative meeting. He asked me to pass on his thanks for setting the meeting up and was encouraging the holding of similar meetings-between ourselves, the divisions and the private sector – whenever appropriate and/or necessary' (RCMP, 2013-05745, p. 220). As the hub for CIP, RCMP members – and O'Neil, in particular – take the responsibility to ensure a continuous watch over potential protests.

Threat entrepreneurs and surveillance of the NEB hearings

In preparation for the NEB public hearings, the joint intelligence working group was lead by the RCMP CIIT. In January 2012, Timothy O'Neil of the CIIT sent an email about the upcoming NEB hearings. He warned that 'there is the possibility that there will be civil unrest and criminal occurrences during the NEB consultation process' (RCMP, 2013-05745, p. 120). He prefaces his email by saying, 'for your general knowledge, I have been tracking credible and potential criminal threats associated to the energy sector for many years now' (RCMP, 2013-05745, p. 130). In providing his assessment, O'Neil's email to a number of other RCMP officers on the issue of upcoming Northern Gateway hearings detailed how the CIIT believe 'environmental extremists pose a significant criminal threat to Canada's energy sector' (RCMP, 2013-05745, p. 130). Underlining that all environmentalists are suspect, O'Neil added that 'many extremists, including those associated to well funded NGOs have the expressed intent and demonstrated capability to engage in criminal activity to prevent and disrupt the development of the Alberta Oil Sands.' O'Neil warns that many 'foreign governments, international

NGOs, academia, and individuals,' routinely 'chastise' Canada for its energy policies. He concludes that 'individuals within this fringe element are possibly inspired and motivated by erroneous information and inflammatory rhetoric – often attributed to credible people – that negatively exaggerates Canada's contribution to climate change' (*ibid*). Unlike contemporary (and increasingly popular) representations that view climate change as endogenous to the market and a catalyst for new opportunities of governance, O'Neil puts forward arguments that cast aspersions on the merits of climate science. In repeating arguments circulated by the climate change 'deniers' movement that is itself a manifestation of the energy lobby (Monbiot, 2006), O'Neil underscores a belief that a 'fringe element' of extremists have commandeered the environmental movement in a false understanding of Canada's environmental policy. These meeting minutes underline the normative bias that informs CIIT's surveillance practices, which is itself a product of the close relations fostered by the petro-security apparatus that we detail below.

As part of the surveillance associated with the Gateway hearings, O'Neil took a lead role in highlighting the possibility of protests around the NEB hearings, and their potentiality toward violence. He wrote that 'it is highly probable that environmental criminal extremists will attempt to mount direct actions targeting Canada's energy sector, specifically the petroleum sub-sector' (RCMP, 2013-05745, p. 131). O'Neil's use of the term 'direct action' is directed to highlight a potential criminal disruption caused by non-violent civil disobedience. For O'Neil, these actions are not associated with democratic conduct, they are criminal opposition to an economic sector he considers crucial to the Canadian economy. We characterize O'Neil's participation in the construction of criminal threats surrounding environment protests as an extension of Becker's notion of moral enterprising. In his study of drug criminalization, Becker (1963) introduced the term of moral entrepreneur to discuss an individual who campaigns relentlessly against social evils. For the construction of eco-threats around the NEB – and in his role in CIP in Canada broadly – O'Neil is a security establishment equivalent to anti-marijuana zealots. O'Neil represents a 'threat entrepreneur' (Mueller, 2006) whose moral enterprising involves labeling environmental activists and critics of the energy industry as deviants. Yet there were no significant criminal events associated with the NEB hearings. While policing agencies might lay claim that surveillance and deterrence strategies could have nullified potential threats, a more likely explanation for the relative orderliness of the demonstrations is that the protesters do not embody the criminal menace circulated by security agencies. Notwithstanding the popular but non-criminal opposition to Gateway, the perspective of a threat entrepreneur holds that being opposed to Gateway is itself construed as deviance and deserving of surveillance.

Impacts of gateway surveillance

In the collection of intelligence related to potential protests around the Gateway proposal, the RCMP has engaged in intelligence sharing with other policing agencies, the NEB's security personnel, CSIS, petroleum firms, and private security firms. RCMP was also involved in distributing intelligence to NEB security officials during the hearings. Appraising the NEB security chief Richard Garber by email on 19 April, 2013, Tim O'Neil noted that the CIIT currently had 'no intelligence indicating a criminal threat to the NEB or its members.' Yet, O'Neil warned that 'anti-oilsands' and 'anti-Canadian petroleum' critics aim for 'the ultimate goal of forcing the shut down of the Canadian petroleum industry' (RCMP, A008929, p. 14). Garber was

assured that 'CIIT will continue to monitor all aspects of the anti-petroleum industry movement to identify criminal activity, and will ensure you are apprized [*sic*] accordingly' (RCMP, A008929, p. 15). O'Neil's language illustrates the scope of activities considered under the banner of CIP. In monitoring 'all aspects of the anti-petroleum industry movement' (we should note that this category of a 'movement' is itself the creation of O'Neil and the RCMP), any expression of opposition toward the energy sector is considered a potential threat to CIP, necessitating investigation by the national security apparatus.

NEB Security Team's engaged in widespread open source surveillance, tracking social media for ruminations of protests targeting the NEB, Gateway, or Enbridge. One email from Garber outlines that the Security Team had conducted 'a thorough review of open source intelligence, including social media feeds.' This circulation of open source surveillance produces a high interest in the mundane. For example, they warn about 'the possibility of activities associated with the 'All Native basketball Tournament' being held in Prince Rupert.' One Situational Awareness report provided to Alberta's Counter-Terrorism Crisis Management Plan (ACTCMP) stakeholders details mundane details of a Hardistry Terminal Protest gathered from intelligence provided by Enbridge (RCMP, A008929, p. 113). Related to an event with an estimated 30–50 people, the threat assessment warns that 'the organizers have indicated the event will be peaceful … traffic will not be impeded as there are no plans for a road blockade' (RCMP, A008929, p. 112). Nonetheless, the intelligence was shared across a network of agencies and corporations. The email concludes that 'this email is to advise you that ASSIST, AEMA, RCMP INSET, RCMP Hardisty and Critical Infrastructure Intelligence National Security Criminal Investigations (Ottawa) are aware of the event' (RCMP, A008929, p. 116). Details are also distributed to a dozen energy companies as well as a private security firm called Torca.

Intelligence is transferred that contains personal information as well. For example, one email from an NEB security officer to Garber, which was forwarded to O'Neil, said: 'Hi John and Rick, I did a little research on the two people who were interviewed by Poor Man Media.' The two individuals' names are clearly visible, even after materials were released under the *Access to Information Act*. The email lists a number of websites where these individuals made critical comments about pipeline development to the media. Another NEB employee, Kelly-Anne Dypolt, sent an email concerning one of the individuals (again, clearly identifiable) under the subject line 'OSI.' The email listed more open source websites, and says 'Found a few things on this fellow' (RCMP, A008929, p. 20). Merely speaking in public about opposition to energy development presents grounds for surveillance efforts. These CIP-inspired surveillance practices are part of a 'security meta-ritual' (Bajc, 2007, p. 1651) drawing together numerous federal security agencies, providing fine-grained details on local conditions and specific individuals deemed to be outsiders.

In addition to open source intelligence, documents demonstrate covert investigations by national security agencies. One email from Garber says that 'the Security Team has consulted today with CSIS at national and regional levels; RCMP at national, regional and local (Prince Rupert Detachment) level.' He concludes his email with the emphasis that 'The Security Team, together with our police and intelligence partners, will continue to monitor *all sources of information and intelligence* and promptly advise the Panel of any changes to the current threat assessment' (RCMP, A008929, p. 37 emphasis added). As Garber underlines, all sources of information were considered germane to the investigation of environmental groups attending the NEB hearings. Based on redaction provisions that were used to exclude materials released under the *ATIA*, the RCMP utilized Section 16(1)(c)(ii) of the *Act* which

excludes information that would 'reveal the identity of a confidential source of information.' Some eco groups have suggested that policing agencies engaged in covert surveillance and infiltration tactics (BCCLA 2014), and this excerpt suggests that is a possibility. In addition to covert tactics, the files indicate that information related to the Board's hearings was being shared between agencies. A number of groups are mentioned, including prominent advocacy groups such as Leadnow, ForestEthics Advocacy, the Council of Canadians, the Dogwood Initiative, EcoSociety, and the Sierra Club of British Columbia. None have any history of violence nor any connection with listed (or unlisted) terrorist organizations. None are criminal organizations, nor do they have any history of financing, advocating, encouraging, or participating in criminal activity.

Notwithstanding, security agencies had decided to utilize 'all sources of information' in an attempt to surveil the 'anti-petroleum movement.' On 31 January 2013, Garber asked personnel to compile 'a high level analyses of the likelihood/potential for aggressive activities' in Prince Rupert NEB hearings (RCMP, A008929, p. 43). Garber then emails RCMP officer V.K. Steinhammer to enquire about potential threats against the Gateway hearings. Steinhammer replies he has 'no intel on hearings' and mentions the possibility of one Idle No More demonstration (*ibid.*). Garber then turns toward more secure information channels and calls 'into CSIS and RCMP Critical infrastructure' (RCMP, A008929, p. 42). Offering a glimpse at the circularity of national security practices, within two hours Steinhammer writes back to Garber and indicates 'This has come back to me to address' (RCMP A008929, p. 41). Having then to itemize the chief national security threat, Steinhammer lists two events of concern: 'The first was during the first round and a female refusing to stop interrupting the proceedings, she was escorted out and shortly after allowed back in with no further interruption. The second was during the last hearings here where there was a small protest over the lunch hour that lasted less than an hour and [was] very peaceful' (RCMP, A008929, p. 41). Steinhammer concludes: 'We have no other information pertaining to any protest or otherwise for the upcoming hearings.'

Despite consistent reporting that no threat is discernible from environmental groups, national security agencies insist on 'monitoring all aspects' of the movement. The surveillance net has expended to include a growing list of groups, who have argued that the surveillance efforts have compromised their abilities to participate fully before the NEB (BCCLA, 2014a; BCCLA, 2014b). The groups have also noted that information sharing between national security agencies and industry representatives may result in information that assists the companies in advancing their position before the NEB, and the 'Board itself may be made privy to unproven yet highly prejudicial allegations against individuals, groups, or organizations' (BCCLA, 2014a, p. 3). In this way, threat entrepreneurialism enacts a normative framework. RCMP characterize environmentalists as 'outsiders,' while industry representatives are colleagues, demonstrating how CIP has become the principle venue for the petro-security apparatus to merge private interests of energy corporations with national security agencies.

Petro policing

Surveillance of environmentalists by Canadian security has resulted in a routine circulation of threat assessments related to critical infrastructure to CIP stakeholders. Circulation of threat assessments has also resulted in institutionalization of intelligence sharing between

security agencies and the energy sector. The energy industry consults regularly with security officials and has the ability to upload its own incident reports directly into RCMP databases, which allows for privately collected intelligence from energy corporations to be aggregated into RCMP national security threat assessments. As a means of integrating the private security arms of the energy sector, SIR databases like SPROS provide more accounts of potential harms to be at the disposal of threat entrepreneurs such as O'Neil. National security databanks such as the SPROS system are key aspects of the CIP surveillance regime and demonstrate how private corporations, and their use of private security intelligence, have become 'deputized' in the field of national security and CIP-oriented surveillance. The contributions and roles of private actors are significant. Indeed, following an August 2010 meeting, 'Ray Fast (E Division) was very concerned that the private sector was receiving intell [*sic*] prior to the [RCMP] Detachments' (RCMP, 2013-05745, p. 220).

Perhaps the most advanced illustration of the petro-security apparatus is the semi-annual Energy and Utility Sector Stakeholder briefings held by CSIS and Natural Resources Canada. Representatives of the energy sector and members of Canada's intelligence and law-enforcement community attend these briefings, conducted at the CSIS headquarters in Ottawa. Energy sector representatives all possess at least Level II (secret) security clearance, allowing them to view classified intelligence. According to the RCMP, the briefings are intended to 'provide intelligence to select energy representatives so they are able to implement the required security precautions to protect their assets' (RCMP, A008499, p. 2). Involving up to 100 participants from public and private sectors, the briefings also 'provide a forum for the private sector to brief the Canadian intelligence and law-enforcement community on issues we would not normally be privy to' (*ibid.*). The principle moderator and organizer of the briefings is the threat entrepreneur Tim O'Neil. An invitee list from May 2011 meetings lists Government of Canada participants as including RCMP, CSIS, DND, Transport, CSE, NEB, Industry Canada, NRCan, Public Safety, AECL, among others. Law enforcement representatives from other provinces (N.B, Alberta, Quebec) were also in attendance. Approximately 50 names are redacted for privacy reasons, likely representing industry and private security personnel. The exclusion of the names of energy company's representatives illustrates the treatment of those regarded as insiders. While the activist 'outsiders' discussed above have their identities searched, cataloged, and released to the public, energy company personnel are protected.

Participants at the Energy and Utility Sector Stakeholder meetings are treated to briefings led by government experts in topics from cyber-security, to economic and corporate espionage. Many of the presentations relate specifically to social movements. For example, after Greenpeace protests targeting nuclear facilities in the Great Lakes region, energy companies were treated to a briefing called 'security challenges presented by radicalized individuals / groups to Canada's energy sector – the Great Lakes examples.' Following confrontational demonstrations against fracking near Elsipogtog First Nation in New Brunswick, a working group held a meeting under the theme 'North American Resource Development at Risk' that featured a number of sessions on potential disruptions presented by social movement actors. These meetings concluded with sessions on suspicious incident reports, and a panel on the 'legal challenges of infrastructure protection: collecting evidence for prosecutions in Canada' (NRCan, 7040-12-214, pgs. 13–17). Meetings in May 2011 included an overview and assessment of Aboriginal Issues of Interest and a session called G8/G20 debriefs. May 2010 meetings included a session on 'Eco-extremism' under G20 updates.

With a focus on two-way intelligence transfers, these meetings also feature round-table discussions on energy sector security with government and industry participants. The meetings entrench the relations and mutual shared values between national security representatives and their security colleagues from the energy sector. The energy sector has also taken steps to contribute to the cordiality of the meetings. Agendas for the meetings in May 2013 (NRCan, 7040-13-094, p. 1) included advertisements that note receptions for the meetings are to be co-hosted by the companies Bruce Power and Brookfield, while breakfast, lunch, and coffee was sponsored by the Gateway pipeline applicant, Enbridge.

An email sent from O'Neil to participants in March 2012 details how the meetings allow for two-way intelligence flows. Addressing Scott Stauffer, from the Canadian Natural Resources ltd Horizon Oil Sands Project,' O'Neil writes: 'Scott, the Oil Sands will continue to be a target for many more years so an assessment from an owner-operator's perspective would be appreciated. Of course, we would welcome your input from your involvement with the Oil Sands Intelligence Working Group' (RCMP, A008499, p. 1). O'Neil concludes by adding: 'The purpose of the panel would be to provide a briefing to the Government of Canada so that it is aware of your initiatives, and secondly and of more value to 'your security peers,' discuss your security procedures, lessons learned, etc' (RCMP, A008499, p. 2). As O'Neil notes, the petro-security apparatus allows RCMP and CSIS to convey how security agencies are defining contemporary and emerging threats and, correspondingly, for private companies to keep the Canadian security establishment apprised of their initiatives.

While RCMP officers like O'Neil present their work as an objective application of criminal law, collaborations under the banner of CIP present an example of the economic interests of the petro state expressed through the risk matrices of police. We emphasize the centrality of human actors, such as O'Neil, in constructing these threats based on moral projections based on the affinities made between the police intelligence services and their 'security peers' within major energy corporations. We refer to these personnel as threat entrepreneurs, and point to how collaborations within the petro-security apparatus produces a community of 'insiders' while self-perpetuating security meta-rituals targeting eco-outsiders.

Discussion and conclusions: Policing and the petro-security apparatus

Aradau (2010) argues that security studies literature has examined discursive aspects of security to the neglect of analyzing how the actual stuff of security matters. She draws attention toward the materials of security projects, specifically critical infrastructure protection since the mid-1990s. Likewise, Lundborg and Vaughan-Williams (2011) argue that the reorientation of security projects based on CIP results in fine-grained security that alters the material of transit ways, and energy networks. While these are useful efforts to draw attention to the materials of security projects, our focus has been the surveillance practices and policing assemblage engendered by the discourse of CIP. As an amalgamation of public and private interests, the surveillance of environmentalists is rationalized through construed threat of protest movements, then shared as intelligence across multiple agencies and private entities. Further, we underline how CIP functions as a 'security trap' (CASE, 2006) that allows for counter-terrorism bureaucracies to extend their mandates, spend allocated resources, and demonstrate a need for future expanded powers given their importance in the face of increasingly asymmetrical threats. As records related to the Gateway hearings show, police and security were concerned about disruptions to critical infrastructure but also debates

about the politics and economics of pipelines. As Deibert and Rohozinski (2010, p. 19) put it, 'disruption to critical infrastructures means, first and foremost, disruption to global capital markets.'

Environmentalists, along with other protest groups – notably indigenous peoples – are now a fixture in intelligence products produced by national security agencies. If individuals are publicly opposed to the energy sector, they will be placed under surveillance by the national security apparatus. The practices of the petro-security apparatus in Canada are noteworthy because of the energy industry's attempts to portray Canadian energy corporations as 'ethical oil.' In keeping with a Canadian myth-making tradition that exalts characteristics of national identity by denigrating others (Thobani, 2007), security authorities have utilized discourses of criminality, and networks of CIP, to construe the environmental movement as a threat to social order. CIP surveillance conflates public dissent with crime and extremism, providing a 'new vocabulary' to constitute a range of public critics as illegitimates and outsiders. A decade of growing CIP resources (and discourses) has normalized a network of state–corporate relationships that now regularly designate protestors as extremists through a disputed allusion to violence, and frames dissenters as outsiders in security meta-rituals (Bajc, 2007) to justify national security state expansion and social movement suppression. This particular state–corporate relationship is strong, and all entities external to that relationship are construed as threatening outsiders. Yet these dissenters are not equal in their outsider status, particularly given Canada's legacy of settler colonialism. Framing rituals of 'Aboriginal extremism' have also arisen in the context of national security policing, particularly with movements that threaten economic interests (Crosby & Monaghan, 2012). Indigenous groups are monitored more closely and on mere suspicion rather than on reasonable, probable grounds. While racialized, stigmatized populations under surveillance are at greater risk of police violence (Comack, 2012; Mitchell & Heynen, 2009) mobilizations against extractive industries illustrate the regularized role of CIP agencies in policing risks to corporate profits.

The Canadian case is yet another example of how CIP-inspired 'counter-terrorism is re-shaping policing and security arrangements…' in Western countries (Palmer & Whelan, 2006, p. 461). CIP-generated surveillance provides an example of 'state-corporate symbiosis' (O'Reilly, 2010) insofar as the connections between private corporate economics and state security agencies are carefully and firmly soldered. We have also used the notion of 'threat entrepreneurs' (also see Sjostedt, 2013) to conceptualize the key role of security personnel in these networks who direct the surveillance practices.

To help theorize this case, we have drawn from Bajc (2007) to suggest that classifying environmental protestors as dangerous to national interests functions to frame dissenters as outsiders in security meta-rituals. The meta aspect of this refers to the emergence of dominant logic used to mitigate uncertainty, make and sort people out as belonging or not in certain social spaces. As she puts it 'This classification is done at the discretion of the security apparatus and without input from the individuals who are being classified. This practice of separation of insiders from outsiders transforms this everyday social life into a security-sanctioned order…' (Bajc, 2007, p. 1670). Persons construed as threats to critical infrastructure and who raise questions about the need for pipelines are categorized as threatening outsiders and targeted for surveillance and future criminalization. Such efforts reflect surveillance and criminalization of social movement groups more generally (see Amster,

2006; Ellefsen, 2012; Fernandez, 2008; Gillham et al., 2013). While they may use threat assessments and positivist language of resilience in their communication with CIP stakeholders, their categorizations are normative and stereotypical, presenting a new vocabulary of threat but maintaining an old grammar of social control. These rituals entail repeated acts of surveillance coordinated by state/federal agencies that target outsiders and block their access to social spaces. They are not allowed to get close to the infrastructure, or even debates about it. Moreover, the unregulated mass accumulation of personal information on protestors in policing databanks raises significant question about the potential use of surveillance intelligence against social movements in the future.

More broadly, we have argued that this new policing assemblage of federal agents and agencies involved in CIP represents a move away from democratic toward regime policing in Canada, demonstrating how the material properties of oil infrastructure in Canada produce the anti-democratic practices of control and suppression. In Canada, the Gateway hearings have concluded and the project has been approved. While numerous requirements have been placed on Enbridge, widespread opposition will continue for the foreseeable future. Given that Gateway is only one among many new energy development projects, the influence of CIP and petro-security apparatus on security practices will increase, which raises concerns regarding the targeting of environmental movements. The categories that these CIP surveillance initiatives utilize conflate social movements with extremism and criminality. These explicit practices of political policing in Canada's petro-security state call the legitimacy of CIP surveillance work into question.

Notes

1. They argue this public–private character is embedded in the National Critical Infrastructure Protection Strategy in Australia as well as in the Critical Infrastructure Protection Program in the US.
2. ASIS International is in its own words the preeminent organization for security professionals. Several chapters are distributed throughout Canada. In February 2014, the Vancouver chapter of ASIS hosted a talk on Assessment for Critical Infrastructure Protection. At a conference in July 2013 in Toronto, there was a seminar entitled 'A Critical Infrastructure Protection Model'.
3. There is also the Canadian Critical Infrastructure Information Gateway operated by Public Safety Canada, which is '…a collaborative, unclassified workspace for the critical infrastructure community.'
4. Canada's Office of Critical Infrastructure Protection and Emergency Preparedness was part of the Department of National Defence before 9/11, but has since been incorporated into the civilian Department of Public Safety.
5. Shadowing government employees may provide the most in-depth data about work in government agencies, and how organizations change over time. However, if shadowing is not possible when dealing with agencies that do not allow researchers entry (such as some security and intelligence agencies), ATI requests present a viable means of producing textual data.
6. These campaigns can be followed by visiting holdthewall.ca, or a campaign site managed by the Council of Canadians, http://canadians.org/enbridge.

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes on contributors

Jeffrey Monaghan is an assistant professor at Carleton University's Institute for Criminology and Criminal Justice. He has a PhD in Sociology from Queen's University. He has published research on a number of areas of policing, security governance, and surveillance. Current research projects include: the globalization of surveillance/security practices and the role of Canadian security experts in exporting these techniques/technologies; the surveillance of social movements with a focus on environmental and indigenous movements; the knowledge construction practices associated with contemporary policing of radicalization; and domestic security governance practices in the context of the 'war on terror.'

Kevin Walby is a chancellor's research chair and an associate professor of Criminal Justice, University of Winnipeg. He is the author of *Touching Encounters: Sex, Work, and Male-for-Male Internet Escorting* (University of Chicago Press 2012). He is co-author with R. Lippert of *Municipal Corporate Security in International Context* (Routledge 2015). He is co-editor of *Brokering Access: Power, Politics, and Freedom of Information Process in Canada* (UBC Press 2012). He has co-edited with R. Lippert *Policing Cities: Urban Securitization and Regulation in the twenty-first Century* (Routledge 2013) and *Corporate Security in the twenty-first Century: Theory and Practice in International Perspective* (Palgrave 2014). He is co-editor of *Access to Information and Social Justice: Critical Research Strategies for Journalists, Scholars and Activists* with J. Brownlee (ARP Books 2015). He is co-editor of *The Handbook of Prison Tourism* with J. Wilson, S. Hodgkinson, and J. Piche (Palgrave 2017). He is co-editor of the *Journal of Prisoners on Prisons* and book review editor for *Surveillance & Society*.

References

Amster, R. (2006). Perspectives on ecoterrorism: catalysts, conflations, and casualties. *Contemporary Justice Review, 9*, 287–301.

Aradau, C. (2010). Security that matters: Critical infrastructure and objects of protection. *Security Dialogue, 41*, 491–514.

Bajc, V. (2007). Surveillance in public rituals: Security meta-ritual and the 2005 U.S. presidential inauguration. *American Behavioral Scientist, 50*, 1648–1673.

Bajc, V. (2013). Sociological reflections on security through surveillance. *Sociological Forum, 28*, 1–9.

BCCLA. (2014a). British Colombia Civil Liberties Association. Letter to Shayna Stawicki, Registrar, Security Intelligence Review Committee. February 6, 2014.

BCCLA. (2014b). British Colombia Civil Liberties Association. Letter to Ian McPhail, Chair, Commission for Public Complaints Against the RCMP. February 6, 2014.

Becker, H. (1963). *Outsiders: Studies in the sociology of deviance*. New York, NY: The Free Press.

Bigo, D. (2006). Internal and external aspects of security. *European Security, 15*, 385–404.

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

Brodeur, J. P. (2010). *The policing web*. New York, NY: Oxford Press.

Canada. (2004a). *Security an open society: Canada's national security strategy*. Ottawa: Government of Canada.

Canada. (2004b). *Government of Canada position paper on a national strategy for critical infrastructure protection*. Ottawa: Public Safety and Emergency Preparedness Canada.

Canada (2009a). *National strategy for critical infrastructure*. Ottawa: Government of Canada.

Canada (2009b). *Action plan for critical infrastructure*. Ottawa: Government of Canada.

CASE. (2006). Critical approaches to security in Europe: A networked manifesto. *Security Dialogue, 37*, 443–487.

Coaffee, J., Murakami-Wood, D., & Rogers, P. (2008). *The everyday resilience of the city: How cities respond to terrorism and disaster*. London: Palgrave.

Collier, S., & Lakoff, A. (2008). The vulnerability of vital systems: How critical infrastructure became a security problem. In Dunn Cavelty, M., & Kristensen, K. (Eds.), *Securing the Homeland: Critical infrastructure, risk and securitisation* (pp. 17–39). London: Routledge.

Comack, E. (2012). *Racialized policing: Aboriginal people's encounters with the police*. Winnipeg: Fernwood Publishing.

Coward, M. (2009). Network-centric violence, critical infrastructure and the urbanization of security. *Security Dialogue, 40*, 399–418.
Crosby, A., & Monaghan, J. (2012). Settler governmentality and the Algonquin of Barriere Lake. *Security Dialogue, 43*, 420–437.
Crosby, A., & Monaghan, J. (2016). Settler colonialism and the policing of idle no more. *Social Justice, 43*(2), 1–21.
Deibert, R., & Rohozinski, R. (2010). Risking security: Policies and paradoxes of cyberspace security. *International Political Sociology, 4*, 15–32.
Dorn, N., & Levi, M. (2009). Private-public or public–private? Strategic dialogue on serious crime and terrorism in the EU. *Security Journal, 22*, 302–316.
Dunn Cavelty, M., & Suter, M. (2008). Early warning for critical infrastructure protection and the road to public-private information sharing. *Intelligencia y Seguridad, 4*, 85–113.
Ellefsen, Rune (2012). Green movements as threats to order and economy? Animal advocates repressed in Austria and beyond. In R. Ellefsen, R. Sollund, & G. Larsen (Eds.), *Eco-global crimes: Contemporary problems and future challenges* (pp. 181–208). Farnham: Ashgate.
Fernandez, L. (2008). *Policing dissent: Social control and the anti-globalization movement*. Chapel Hill: Rutgers University Press.
Gillham, P., Edwards, B., & Noakes, J. A. (2013). Strategic incapacitation and the policing of Occupy Wall Street protests in New York City, 2011. *Policing and Society, 23*, 81–102.
Godfrey, R., Brewis, J., Grady, J., & Grocott, C. (2014). The private military industry and neoliberal imperialism: Mapping the terrain. *Organization, 21*, 106–125.
Harris, C. (2004). How did colonialism dispossess? Comments from an edge of empire. *Annals of the Association of American Geographers, 94*, 165–182.
Howe, Miles (2015). *Debriefing Elsipogtog: The anatomy of a struggle*. Halifax: Fernwood.
Kinsman, G., Buse, D., & Steedman, M., (Eds.). (2000). *Whose national security? Canadian state surveillance and the creation of enemies*. Toronto: Between the Lines.
Kinsman, G., & Gentile, P. (2010). *The Canadian war on queers: National security as sexual regulation*. Vancouver: UBC Press.
Koski, C. (2011). Committed to protection? Partnerships in critical infrastructure protection. *Journal of Homeland Security and Emergency Management, 8*, 1–19.
Kulchyski, P. (2013). *Aboriginal rights are not human rights. In defence of indigenous struggles*. Winnipeg: ARP Books.
Lentzos, F., & Rose, N. (2009). Governing insecurity: Contingency planning, protection, resilience. *Economy and Society, 38*, 230–254.
Lipschutz, R. (2008). Imperial warfare in the naked city—Sociality as critical infrastructure. *International Political Sociology, 2*, 204–218.
Lubbers, E. (2012). *Secret manoeuvres in the dark corporate and police spying on activists*. London: Pluto Press.
Lundborg, T., & Vaughan-Williams, N. (2011). Resilience, critical infrastructure, and molecular security: The excess of "life" in biopolitics. *International Political Sociology, 5*, 367–383.
McCreary, T., & R. Milligan. (2014). Pipelines, permits, and protests: Carrier Sekani encounters with the Enbridge Northern Gateway Project. *Cultural Geographies, 21*, 115–129.
McDiarmid, M. (2014). Environmentalists shift focus to more grassroots, less government. *CBC News*. October 3.
Mitchell, D., & Heynen, N. (2009). The geography of survival and the right to the city: Speculations on surveillance, legal innovation, and the criminalization of intervention. *Urban Geography, 30*, 611–632.
Monahan, T., & Palmer, N. (2009). The emerging politics of DHS fusion centers. *Security Dialogue, 40*, 617–636.
Monbiot, G. (2006). *Heat: How to stop the planet from burning*. Toronto: Doubleday Canada.
Mueller, J. (2006). *Overblown: How politicians and the terrorism industry inflate national security threats, and why we believe them*. New York, NY: Free Press.
Newbold, K., Jr, & Delp, B. (2011). Critical infrastructure protection program: A case study on higher education collaboration in homeland security. *The Homeland Security Review, 5*, 193–212.
Nikiforuk, A. (2001). *Saboteurs: Weibo Ludwig's war against big oil*. Toronto: Macfarlane Walter and Ross.

O'Reilly, C. (2010). The transnational security consultancy industry: A case of state-corporate symbiosis. *Theoretical Criminology, 14*, 183–210.
Palmer, D., & Whelan, C. (2006). Counter-terrorism across the Policing Continuum. *Police Practice and Research, 7*, 449–465.
Potter, W. (2011). *Green is the New Red: An insider's account of a social movement under siege*. San Francisco: City Lights.
Pynnöniemi, K., & Busygina, I. (2013). Critical infrastructure protection and Russia's hybrid regime. *European Security, 22*, 559–575.
Quigley, K. (2013). "Man plans, God laughs": Canada's national strategy for protecting critical infrastructure. *Canadian Public Administration, 56*, 142–164.
Sjostedt, R. (2013). Ideas, identities and internalization: Explaining securitizing moves. *Cooperation and Conflict, 48*, 143–164.
Stake, R. (1995). *The art of case study research*. Thousand Oaks: Sage.
Thobani, S. (2007). *Exalted subjects*. Toronto: University of Toronto Press.
Walby, K., & Monaghan, J. (2011). Private eyes and public order: Policing and surveillance in the suppression on animal rights activists in Canada. *Social Movement Studies, 10*, 21–37.
Whitaker, R., & Marcuse, H. (1994). *Cold war Canada: The making of a national insecurity state, 1945–1954*. Toronto: University of Toronto Press.

Access to Information Act Requests

CSIS (Canadian Security Intelligence Service). 2009-143. *Access to information Act* request.
NRCan (Natural Resources Canada). 7040-12-214. *Access to information Act* request.
NRCan (Natural Resources Canada). 7040-13-094. *Access to information Act* request.
PSC (Public Safety Canada). 2009-00280. *Access to information Act* request.
RCMP (Royal Canadian Mounted Police). A008499. *Access to information Act* request.
RCMP (Royal Canadian Mounted Police). A008929. *Access to information Act* request.
RCMP (Royal Canadian Mounted Police). 2013-05745. *Access to information Act* request.
RCMP (Royal Canadian Mounted Police). 2013-013180. *Access to information Act* request.
RCMP (Royal Canadian Mounted Police). 2012-016333. *Access to information Act* request.
RCMP (Royal Canadian Mounted Police). 2011-016328. *Access to information Act* request.