Infrastructures of Pacification: Vital Points, Critical Infrastructure, and Police Power in Canada

Philip Boyle and Tia Dafnos*

Abstract

Though described as the first milestone towards securing Canada's critical infrastructure (CI), the 2009 National Strategy for Critical Infrastructure is the most recent effort in decades of federal engagement with the problem of how to secure the material elements that underpin state, economy, and society. In this article, we show how a little-known civil defence program initiated after WWII to protect important industrial facilities from military enemies has transformed in the contemporary period into the monitoring of a range of political and social movements as perceived dangers to what is understood today as CI. We view these changes as indicative of transformations in the exercise of police power through which the contemporary colonial-liberal order is enacted.

Keywords: police, security, critical infrastructure, security intelligence, pacification

Résumé

Bien qu'elle soit décrite comme le premier jalon de la sécurisation des infrastructures essentielles du Canada (CI), la Stratégie nationale sur les infrastructures essentielles de 2009 ne représente que l'effort le plus récent, au fil de décennies d'engagement fédéral, sur la question de la sécurisation des éléments matériels qui sous-tendent l'État, l'économie et la société. Dans cet article, nous illustrons comment un programme peu connu de défense civile, initié après la Seconde Guerre mondiale, visant à protéger les installations industrielles importantes des militaires ennemis s'est transformé au cours de la période contemporaine en une surveillance d'une série de mouvements politiques et sociaux qui sont perçus comme un danger vis-à-vis de ce qui est compris aujourd'hui comme une CI. Nous analysons ces changements à titre d'indicateurs de transformations dans l'exercice du pouvoir de police à travers lequel l'ordre colonial-libéral contemporain est promulgué.

Mots clés : police, sécurité, infrastructure critique, intelligence sécuritaire, pacification

* Philip Boyle acknowledges support for this research from the Social Sciences and Humanities Research Council of Canada. Tia Dafnos acknowledges support for research used in this article from the Harrison McCain Foundation and the Social Sciences and Humanities Research Council of Canada. The authors would like to thank Eric Reiter and two anonymous reviewers for commenting on previous versions of this article.

Canadian Journal of Law and Society / Revue Canadienne Droit et Société, 2019, Volume 34, no. 1, pp. 79–98. doi:10.1017/cls.2019.5

Police and the Pacification of Infrastructure

The security of critical infrastructure (CI) systems seems to have emerged in the last two decades as a leading security concern for advanced liberal democracies.[1] Much of this concern came in the immediate aftermath of 9/11, an event that underscored the vulnerability of complex and large-scale infrastructure systems to even low-tech actors with malicious intent. Reinforced by events such as the 2003 Canada/US electrical grid failure and the train bombings in Madrid (2004) and London (2005), countries across the global north rushed to protect essential but fragile CI. In Canada the federal government responded to these concerns by adopting the *National Strategy for Critical Infrastructure* in 2009. The main premises of the *National Strategy* are as follows: first, Canada's CI is vulnerable to a wide range of malicious threats (i.e., terrorism and criminal extremism) and non-malicious hazards (e.g., ice storms, floods, or industrial accidents); second, the vast majority of Canada's CI is owned by private sector actors and/or different levels of government, and responsibility for CI protection is therefore distributed across a diverse range of actors; and third, the federal government, through Public Safety Canada, should play a coordinating role amongst these actors to "prevent, mitigate, prepare for, respond to, and recover from disruptions of critical infrastructure and thereby safeguard the foundations of our country and way of life."[2]

Though described as "the first milestone," the *National Strategy* is the most recent effort in decades of federal engagement with the problem of how to secure the material elements that underpin post-war Canada.[3] In this article, we examine one particular strand of this engagement by focusing on the role of the RCMP in governing what were referred to during the Cold War as "vital points," which was a designation used to indicate important industrial production and supply facilities necessary to mobilize for war. We begin by showing how the RCMP played an integral role in developing national plans for the protection of vital points in the early years of the Cold War that were to be implemented alongside other internal security measures upon invocation of the *War Measures Act* (WMA). A consistent, if amorphous, motivation for these efforts was the apparent threat of sabotage to vital points by covert Soviet forces or Communist sympathizers operating inside the country. One of the main objectives of this article is to show how the protection of vital points from military enemies has transformed in the contemporary period into the monitoring of a range of political and social movements on the

[1] The article draws on open source material, documents obtained through Access to Information (ATI) requests, and interviews. ATI request numbers have been included for all documents cited. Historical material on the vital points program was obtained by ATI from Library and Archives Canada from the following collections: Emergency Preparedness Canada (RG 57), Transport Canada (RG 12), Aerospace, Defence, and Industrial Benefits Canada, Department of National Defence (RG 24), Department of Foreign Affairs (RG 25). Archival material was also obtained from the Department of National Defence (DND) Headquarters Directorate of History and Heritage.

[2] Public Safety Canada, *National Strategy for Critical Infrastructure* (Ottawa: Public Safety Canada, 2009), 3.

[3] Ibid.; see also Philip Boyle and T Shannon. Speed, "From Protection to Coordinated Preparedness: A Genealogy of Critical Infrastructure in Canada," *Security Dialogue* 49, no. 3 (2018): 217–31.

https://doi.org/10.1017/cls.2019.5 Published online by Cambridge University Press

basis of the perceived dangers they pose to what is now understood to be "critical infrastructure."[4] Yet our aim is not simply to detail a history of how *old* security threats have come to be conflated with a range of *new* security threats to comprise a "heterogeneous field of menace" that security actors must now confront.[5] Instead, we provide a genealogy of the preceding discursive and socio-legal transformations that have made such conflations institutionally possible. In particular, we show how security intelligence came to be embraced in the 1990s as a solution for the inadequacies of inherited Cold War-era policies and institutionalized in new intelligence networks anchored by the RCMP. A notable feature of these networks is the aim of enhancing coordination and information-sharing between the RCMP and the private sector owners and operators of CI across Canada. Intelligence work is typically considered to be the preserve of the state, yet this intelligence network exhibits a high degree of strategic and operational alignment between the RCMP and the in-house security outfits of private CI owner-operators as it matures. Below we show how these connections arise from a discursive reformulation of vital points into the contemporary notion of CI in the late 1990s and an expansive understanding of risk to constitute an expanding intelligence apparatus in which crime, terrorism, and political protest, amongst other activities, can be conflated as threats to the liberal *way of life*.

The wider dynamics that our investigation illuminates are not the civilianization of military concerns or the creeping militarization of civilian governance. Nor is this a story of scope creep in which longstanding security programs have simply broadened over time. In our view, our analysis is about transformations in the operations of power at work in the fabrication of the liberal social, political, and economic order. For Neocleous, the economic and political order of liberalism "is not a spontaneous order" but an ongoing accomplishment enabled by the operations of a particular form of power: police power.[6] Here, Neocleous is recovering the older and broader meaning of "police" found in the eighteenth century city-states of the German territories characterized by extensive and intensive regulations on collective life in the name of promoting "good welfare and the condition of good order."[7] Foucault has shown how the vast and detailed regulatory reach of eighteenth-century police would later be problematized by early liberal thinkers for exemplifying the tendency for state overreach when contemplating the proper limits of state power.[8] But concern with the political administration

---

4 Tia Dafnos, "Pacification of Indigenous Struggles in Canada," *Socialist Studies* 9, no. 2 (2013): 57–77; Tia Dafnos, Scott Thompson, and Martin French, "Surveillance and the Colonial Dream: Canada's Surveillance of Indigenous Protest," in *National Security, Surveillance, and Terror: Canada and Australia in Comparative Perspective*, ed. Kevin Walby, Randy Lippert, Ian Warren, and Darren Palmer (Basingstoke: Palgrave-MacMillan, 2016), 319–42; Jeffrey Monaghan and Kevin Walby, "Surveillance and Environmental Movements in Canada: Critical Infrastructure Protection and the Petro-Security Apparatus," *Contemporary Justice Review* 20, no. 1 (2017): 51–70; Shiri Pasternak and Tia Dafnos, "How Does a Settler State Secure the Circuitry of Capital?," *Environment and Planning D: Society and Space* 36, no. 4 (2018): 739–57.

5 Monaghan and Walby, "Surveillance and Environmental Movements," 52.

6 Mark Neocleous, "'A Brighter and Nicer New Life': Security as Pacification," *Social & Legal Studies* 20, no. 2 (2011): 191–208.

7 Mark Neocleous, *War Power, Police Power* (Edinburgh: University of Edinburgh Press, 2014), 30.

8 Michel Foucault, Security Territory, *Population* (New York: Picador, 2007).

https://doi.org/10.1017/cls.2019.5 Published online by Cambridge University Press

of "good order" did not simply disappear with the invention of the biopolitical practices of liberalism.[9] To the contrary, police power continues to be an operative form of power through which the liberal order is structured and enforced, the inherent violence of which is masked when carried out in the name of "security." From this perspective, security is therefore better understood as *pacification,* in which police power is active in producing *particular kinds* of order through the suppression of populations, relations, and activities deemed to be "out of order."

We view the governance of infrastructure as a key plane for the exercise of police power in the fabrication of the contemporary liberal order. What is recognized today as CI "protection" or CI "security," in other words, is a pacification project with deep roots in the founding and enforcement of liberalism as a political project. Indeed, infrastructures *themselves* are already pacification projects in a dual sense: the material laying of infrastructure is a modality of pacification that overwrites inherited social, political, and economic activities and spaces with new geometries of power while simultaneously enabling the circulation of agents of state surveillance and control to monitor national frontiers distant from the centres of colonial power.[10] Strategies to secure the same infrastructure can thus be seen as a form of *reflexive* pacification insofar as they envelop the very instruments of pacification with a second-order laminate of police power that operates to smooth out potential disruptions to the material foundations of capital accumulation.

Our analysis is foundationally about transformations in the ensemble of mechanisms through which police power—understood as the power to fabricate order/pacify disorder—operates in relation to the material elements of exchange and circulation in post-war Canada. As we show below, throughout much of the Cold War period, this exercise of police power derived from the wartime emergency powers of the federal government and took the form of vast and secret taxonomies of industrial systems and their vulnerabilities. Today, the exercise of police power no longer derives from exceptional emergency power and nor does it take the form of "endless lists and classifications" that is characteristic of police power.[11] Instead, the exercise of police power today is accomplished through the "normal" powers of the federal government and operates by extending surveillance in the form of "security intelligence" on domestic populations deemed to threaten advanced liberal visions of economic order. Decoupling the mechanisms of police power from exceptional emergency power and the needs of industrialized warfare is a relatively recent shift in governance that has had the paradoxical effect of radically extending the surveillance of domestic populations in ways that

[9] Neocleous, *War Power*; Markus Dubber and Mariana Valverde, *The New Police Science: The Police Power in Domestic and International Governance* (Stanford, CA: Stanford University Press, 2006); Mark Neocleous, *Critique of Security* (Toronto and Montreal: McGill-Queen's University Press, 2008).

[10] Laleh Khalili, "The Roads to Power: The Infrastructure of Counterinsurgency," *World Policy Journal* 43, no. 1 (2017): 93–99.

[11] Colin Gordon, "Governmental Rationality: An Introduction," in *The Foucault Effect: Studies in Governmentality*, ed. Burchell Graham, Colin Gordon, and Peter Miller (Chicago: The University of Chicago Press, 2001), 10.

are routine, ongoing, and mostly consistent with liberal rule. How and under what conditions this shift occurred is the focus of this article.

The Political Administration of Circulation

We begin this article with the observation that, despite the apparent newness with which concerns about CI were articulated in the late 1990s and early 2000s, the protection of "vital," "critical," or "essential" networks is a problem that is intrinsic to the political administration of life itself. Foucault has examined how, in the context of "resistances, revolts, and insurrections of conduct" of the eighteenth century, the early modern arts of liberal governance emerged in response to the new question of "how things should circulate or not circulate."[12] Taking the "fine materiality of human existence and coexistence, of exchange and circulation" found in the early modern town as the crucible of the problem, Foucault analyzed the emergence of strategies capable of "allowing circulations to take place, of controlling them, sifting the good and the bad, ensuring that things are always in movement, constantly moving around, continually going from one point to another, but in such a way that the inherent dangers of this circulation are cancelled out."[13]

Foucault diagnosed how the problem of managing circulation became a "privileged object for police."[14] This form of early-modern statecraft concerned itself not only with the numbers, health, and living conditions of subject-citizens of the state but also with the "space of circulation" in which people and things were embedded.[15] Foucault characterized the space of circulation as the "milieu," itself composed of "natural givens—rivers, marshes, hills—and a set of artificial givens—an agglomeration of individuals, of houses, etc."[16] While biopolitical strategies developed in relation to the discovery of the population and its statistical regularities, the material elements composing the milieu of circulation continued to be an object and target for police administration. "Thus, police will be concerned with the condition and development of roads, and with the navigability of rivers and canals, etc."[17] Gradually the political technologies of police developed into highly detailed regulations and urban ordinances through which the problems of dense coexistence and circulation could be managed not only to immunize the state from insurrection but to organize the spaces and relations of production of the emerging liberal and capitalist order.[18]

In the nineteenth and twentieth centuries, the utopian dream of the well-ordered town was transposed to the level of the nation-state, making the state "into a sort of big town, arranging things so that the territory is organized like

12 Foucault, *Security, Territory, Population*, 28, 64.
13 Ibid., 339, 65.
14 Ibid., 325.
15 Ibid., 326.
16 Ibid., 21.
17 Ibid., 325.
18 Michael Dillon and Julian Reid, *The Liberal Way of War: Killing to Make Life Live* (London and New York: Routledge, 2009).

https://doi.org/10.1017/cls.2019.5 Published online by Cambridge University Press

a town, on the model of a town, and as perfectly as a town."[19] This vision underpinned the development of national infrastructures that became the backbone and lifeblood of capitalist nation-states and of global trade. From roads, rivers, canals, and grain stores to railways and electrical grids, the development of national infrastructures extended the foundation for the contemporary liberal and capitalist order by enabling access to—and mobility of—land, resources, labour, and markets. But beneath the modernist vision of the well-ordered nation bound by national infrastructure lies a far messier reality: infrastructures break, corrode, and fail; they are vulnerable to disruption from weather, animals, and accidents; infrastructures are targeted as symbols of rule by distant colonial powers, easily downed by labour disputes, and predictably fail in unpredictable ways due to their own complexity.[20] Moreover, by the early twentieth century, it was recognized that the material networks developed to enhance the biopolitical vitality of the population were prone to fail in potentially catastrophic ways, introducing new sources of vulnerability to human populations that required intervention. These problems introduced a new and reflexive concern with *systems vulnerability* to the project of biopolitical modernity that Collier and Lakoff have referred to as vital systems security. Whereas the "classical" mechanisms of biopolitical security emerging in the eighteenth century enframed human populations as objects to be known and governed, systems vulnerability emerged in the twentieth century as a problem-space for government action in relation to the vital but vulnerable instruments of circulation on which biopolitical modernity had come to depend.[21]

The RCMP and Industrial Security During the Cold War

Far from being displaced by the biopolitical strategies of liberalism, the emergence of systems vulnerability as a distinct problem-space in the early twentieth century assured that the exercise of police power would remain a feature of contemporary liberal governmentality. In the late 1800s, police-like powers were already being exercised by the colonial government to organize trade and monitor Indigenous populations in post-Confederation Canada.[22] In the mid-twentieth century, the needs of industrialized warfare reoriented and consolidated the fragmentary exercise of police power into a flexible and mutable framework established to secure civilian industrial facilities necessary to mobilize for war. These efforts derived

19 Foucault, *Security, Territory, Population*, 226.

20 Stephen Graham and Nigel Thrift, "Out of Order: Understanding Repair and Maintenance," *Theory, Culture & Society* 24, no. 3 (2007): 1–25; Stephen Graham, ed., *Disrupted Cities: When Infrastructure Fails* (London and New York: Routledge, 2010).

21 Stephen Collier and Andrew Lakoff, "The Vulnerability of Vital Systems: How 'Critical Infrastructure' Became a Security Problem," in *Securing "The Homeland": Critical Infrastructure, Risk and (In)Security, Political Perspectives* (London and New York: Routledge, 2008); Stephen Collier and Andrew Lakoff, "Vital Systems Security: Reflexive Biopolitics and the Government of Emergency," *Theory, Culture & Society* 32 no. 2 (2015): 19–51.

22 Jeffrey Monaghan, "Settler Governmentality and Racializing Surveillance in Canada's North-West," *Canadian Journal of Sociology* 38, no. 4 (2013): 487–508; Mariana Valverde "'Peace, Order, and Good Government': Policelike Powers in Postcolonial Perspective," in *The New Police Science: The Police Power in Domestic and International Governance* (Stanford, CA: Stanford University Press, 2006), 73–106.

https://doi.org/10.1017/cls.2019.5 Published online by Cambridge University Press

from the Internal Security provisions of the federal War Book of 1948 that were to come into effect upon declaration of a national emergency under the WMA. Alongside general measures such as controlling ships, aircrafts, and essential supplies, the War Book assigned the Minister of Justice (and thus the RCMP) specific responsibilities for countering subversion by identifying and detaining persons considered to be "dangerous to the safety of the State," as well as for the protection of vital points, which it defined as "an administrative or industrial establishment that is essential to the prosecution of a war effort or to the maintenance of basic economic life, and for which there is no satisfactory alternative."[23] Modeled as they were on the British system, these responsibilities were to be operationally distinct within the RCMP, thus introducing a distinction between the security and emergency/protective service branches of the service that would be entrenched in the decades to follow.[24]

In light of the responsibilities assigned by the War Book, the RCMP embarked on an elaborate program of industrial security in 1948 that spanned much of the Cold War. These efforts formed a considerable but lesser-known component of the agency's efforts to combat the "fifth column" of Soviet operatives thought to be active in Canada at the time.[25] In one sense, the protection of vital points was an obvious area for extending the RCMP's efforts because industrial labour unions were seen to be susceptible to Communist infiltration. At the same time, however, the protection of vital points was viewed as something conceptually distinct from the RCMP's other internal security programs and those of other federal entities—a problem unto itself rather than simply a new theatre to pursue Communists. An RCMP memo from the early 1950s describes this new domain as such: "This is a matter separate from civil defence, which is concerned with the protection and provision of assistance to the civil population, and the protection of property generally against the effects of an enemy attack. The problem I am referring to is related solely to essential services—transportation, electrical power, manufacturing, etc."[26]

Just as the seventeenth- and eighteenth-century *Polizeiwissenschaft* carved out a sphere of expertise in relation to circulation in the early modern towns of the German territories, so too did the RCMP carve out a new area of expertise as regulators of industrial security during the Cold War.[27] This consisted of two main sets of activities for the RCMP: first, arranging for the physical protection of the most important vital points—those designated as Category I by an inter-departmental steering committee—under invocation of the WMA; and second, to inspect and

[23] War Book, Chapter III—Internal Security Measures. Privy Council Office. September 1948. LAC RG57-B-1, vol. 4, book no. 87. A-2015-00053.

[24] Lawrence Aronsen "'Peace, Order and Good Government' during the Cold War: The Origins and Organisation of Canada's Internal Security Program," *Intelligence and National Security* 1, no. 3 (2008): 357–80.

[25] See Reg Whitaker and Gary Marcuse, *Cold War Canada: The Making of a National Insecurity State, 1945–1957* (Toronto: University of Toronto Press, 1994).

[26] Memo from Commissioner Nicholson to provincial Attorneys General (n.d.). From context and placement in files this memo was likely produced in 1951. LAC RG 57, A-2015-00053.

[27] Franz-Ludwig Knemeyer, "Polizei," *Economy and Society 9*, no. 2 (1980): 172–96.

https://doi.org/10.1017/cls.2019.5 Published online by Cambridge University Press

advise on physical security for all listed vital points outside of war. Agreements with the Armed Forced enabled the RCMP to share responsibility for protecting Category I vital points during war for up to six months. Under these agreements, plans for the protection of vital points were coordinated by the same joint committee also responsible for the more infamous internment operations carried out under the WMA. From an operational standpoint, keeping saboteurs *out* of vital points and foreigners *inside* internment camps were logistically inverse but equivalent operations that could be planned together and carried out as one.[28]

The second set of activities—inspecting and advising industrial facilities on emergency protective measures to be implemented by owner/operators themselves under declaration of war—constituted a much more active component of the program for the RCMP. In the decades after 1951, the agency conducted hundreds of security inspections and produced countless pages of inspection reports on industrial and administrative facilities across the country. The advent of intercontinental missiles in the late 1950s that could deliver atomic weapons with little warning raised the question of whether it was useful to continue with such highly localized efforts, but updated military assessments concluded that sabotage remained probable after the initial phase of nuclear war in an attempt to delay recovery operations.[29] The field surveys conducted by the RCMP expanded in the 1960s to include energy, communication, and transportation networks determined to be essential for post-strike evacuation and continuity of government operations. The entire St. Lawrence Seaway was identified as offering "unlimited electronic possibilities to the enemy to monitor our communications, planting aids to guided missiles, or stockpiling delayed action bombs," and in 1961, the RCMP set about a survey of the seaway in preparation for post-strike recovery operations.[30]

The FLQ crisis in 1970 radically expanded the already stretched capabilities of the RCMP with respect to vital points. Famously, the FLQ crisis is the only time outside of WWI and WWII that the WMA was invoked, yet nearly two decades of preparation were found to be inadequate for countering the low-grade guerrilla tactics the FLQ were known for when the act was invoked in the fall of 1970. A situation assessment put together in the immediate aftermath of the crisis concluded that these tactics were the forbearers and lifeblood of future "revolutionary wars" in which small groups of subversives would infiltrate civil institutions such as churches and political organizations, then escalate to "attacks on the systems upon which civil society depends," such as "communication systems and supporting services," "power source systems—hydro, thermal, gas, etc.," and "transportation systems—ground, air, and water," culminating in "all-out warfare against

[28] Army Committee on Internship Operations & Vital Points, RCMP-Army Plan for Vital Points, December 18, 1950. LAC RG 24, A-2015-00168.

[29] Memo to J. K. Starnes, Chairman, Joint Intelligence Committee, Department of External Affairs, from J. C. Morrison, Acting Chairman, Interdepartmental Committee on Vital Points, January 20, 1960. Response to Morrison from Starnes, February 18, 1960. LAC RG 57, A-2015-00053.

[30] Memo to R. B. Curry, Director, Emergency Management Organization, re: Security Surveys—St. Lawrence Seaway, from G. W. Mudge, OIC, Emergency Planning Branch, RCMP, July 4, 1961. LAC RG 57, A-2015-00053.

Government Armed Forces with the intent to take-over national and local governments and establish a revolutionary government."[31] Informed by this forecast, the federal government directed a second, "Vital Points (Peace)," program to be administered alongside the "Vital Points (War)" program. Whereas the existing war program continued to define a vital point in terms of prosecuting or recovering from war against military enemies, the demands of armed conflict are conspicuously absent from the new program; instead, a "vital point" was defined as any facility "essential for government operations, the economy, or the morale of the population."[32]

For the RCMP, the predictable effect of administering a second vital points program with vastly broader terms was an exponential increase in the scope and complexity of the field inspections under the program during the 1970s. After thirty years of on-and-off updating, the war list contained just under 1,000 facilities by the mid-1970s, while the peace list, initiated in 1971 with a few dozen government buildings in Ottawa and Montreal, topped 6,000 points within seven years. The sheer number of listed facilities was further complicated by hardening jurisdictional disputes between Ottawa and the provinces that forced the RCMP to manage war and peace lists for facilities under federal jurisdiction as well as war and peace lists for each province, leading to thousands of listings distributed across twenty-two working ledgers near the end of the decade. To streamline the situation, the federal government dissolved the war and peace distinction in 1979, reasoning "most vital points have the same significance and require the same protection whether the country is at war or in a state of civil unrest," and reorganized the entire pool of vital points according to federal and provincial jurisdiction.[33] These changes stabilized the federal vital points lists to fewer than one hundred Category I vital points and several hundred lower-priority listings by the middle of the 1980s.

The decade-long experiment with parallel vital points programs foreshadows the reorientation of police power away from external military enemies towards a broader range of politically-motivated "subversives" as well as the downgrading of war amongst the factors determining what was "vital" to the nation. Nevertheless, plans for the protection of vital points remained formulated with the intent of being "stood up" and "wound down" upon invocation and revocation of a national emergency under the WMA. While the RCMP worked with owner/operators of vital points to develop emergency protection plans for much of the Cold War, implementation of those plans was nevertheless contingent upon such a declaration (as well as upon the willingness of owner/operators to do so, which the RCMP seemed to regard as a dubious assumption). Similarly, the RCMP's own plans to protect Category I vital points necessitated the declaration of a national emergency to become operational.

---

[31] Analysis of Target Selection During Revolutionary War, January 5, 1971. LAC RG 12, A-2015-00114.

[32] Memo to Cabinet, Re: Protection of Vital Points, December 14, 1970. LAC RG 12, A-2015-00114.

[33] Peacetime Vital Points, September 26, 1979. LAC RG 12, A-2015-00114.

In the mid-1980s an external review of the vital points program (the "Geddes review") concluded that the emphasis on time-limited emergency protection was insufficient in light of what it warned to be the coming era of "computer crime, mass destruction terror, and mind manipulating communications."[34] The review recommended that Emergency Preparedness Canada (EPC)—which was then overseeing the program—shift from encouraging temporary emergency protection to fostering an "ongoing state of physical protection" amongst the owner/operators of vital points. Rather than providing direct financial assistance for this ongoing state of security, it encouraged EPC to develop a range of information products to entice and guide investments in security on the part of owner/operators.[35] The provision of accurate and up-to-date intelligence on threats to vital points was envisioned as one form of such support, yet the review also noted that there was practically no institutionalized capacity to provide such intelligence to the private sector owner/operators of vital points: "The main limitation in the Canadian Vital Points Program is the practice of self-help, amateur security intelligence estimates. It provides a dangerous base for the contingency planning of the protection of the nation's vital points and must be replaced by professional security intelligence processes."[36]

The review consequently recommended the creation of a dedicated "security estimate" to provide information on the status of threats to vital points tailored to specific industrial sectors and geographic regions. "In time, the estimate should deal with specific targets such as pipelines, air transportation systems, computer systems, telecommunications systems, etc. so that their vulnerability can be assessed in relation to the threat as a basis for updating the contingency protection plans."[37] The McDonald Commission came to a similar conclusion in its review of the RCMP's Security Service. Noting that the Security Service had failed to provide useful advice on the threat of sabotage to vital points, it recommended that its proposed intelligence agency (after 1984, CSIS) "should be responsible for reporting intelligence on new targets of terrorists or saboteurs to the Advisory Committee on Vital Points."[38]

The critiques of the Geddes review and McDonald Commission are early signals of the embrace of security intelligence to come in the 1990s. But rather than being installed as an add-on to existing practices as envisioned by the Geddes review and the McDonald Commission, security intelligence would instead be positioned as a key regulatory mechanism within a wider political and discursive reconceptualization of "vital points" into the contemporary object that is "critical infrastructure." Below we show how this reformulation necessitated adopting new strategies for governing this "new" object of national security.

---

34 R. R. Geddes, *Protecting Category II Vital Points During Time of War or Serious Civil Crisis* (Ottawa: Emergency Preparedness Canada): Summary.
35 Ibid., 76.
36 Ibid., 4.
37 Ibid., 32.
38 *Royal Commission of Inquiry into Certain Activities of the RCMP* (Ottawa: Commissions of Inquiry, 1981): Report 2, Vol. 2, Part IX, Para 86.

https://doi.org/10.1017/cls.2019.5 Published online by Cambridge University Press

From Vital Points to Critical Infrastructure

Before the 1990s, the notion of infrastructure was largely absent from security and political discourses in Canada. The 1994 National Defence White Paper, for example, which set out a range of future security challenges that the Department of National Defense would need to prepare for (such as overpopulation, uncontrolled migration, environmental degradation, and state-sponsored terrorism), makes no mention of domestic infrastructure as a future security priority. Infrastructure is similarly absent from Canada's Security Policy at the time, and from the RCMP's 1994 Guide to Threat and Risk Assessment for Information Technology.

Amongst other countries of the North Atlantic, however, concerns about the extent to which the well-being of the population and governments relied on vital but vulnerable systems were increasingly being articulated through the idea of "critical infrastructure" by the 1990s. Historically, the term "infrastructure" was used by international organizations such as NATO to refer to military installations and assets, and by the World Bank to refer to material works seen as essential to "international development."[39] In the 1970s, the term took on wider usage in the context of the "logistics revolution," as global industries adopted principles from the military art of logistics and supply to reconfigure practices into a "just-in-time" mode of production and distribution based on "optimized" supply chain management.[40] From there, the term diffused to wider technoscientific and political discourses, where the more specific idea of *critical* infrastructure emerged, particularly in the United States and amongst European countries, as a seemingly generic reference to facilities, systems, networks, and services essential to a nation.[41] At the same time, "critical infrastructure" also served as a useful designation for a constellation of concerns that the complexities and interdependencies of infrastructure systems—driven by population growth, technological advances, and the liberalization of global markets—would compound the effects of infrastructure disruptions to produce catastrophic outcomes for economic systems and, by extension, human populations. These were, of course, not entirely new concerns, but the growth of "just-in-time" logistical economies and the neoliberal diversification of infrastructure ownership from the 1970s onward were seen to accentuate the problem of radical contingency and catastrophic disruption intrinsic to the longstanding problem of systems vulnerability.[42]

Governmental discourse in Canada, however, retained the ontology and epistemology of the vital points program well into the 1990s. Even after the WMA was repealed, emergency planners in EPC concluded that planning for the protection

---

39 Ashley Carse, "Keyword: Infrastructure. How a Humble French Engineering Term Shaped the Modern World," in *Infrastructures and Social Complexity: A Companion*, ed. P. Harvey, C. Brunn Jensen, and A. Morita (New York: Routledge, 2016), 27.

40 Deborah Cowen, *The Deadly Life of Logistics. Mapping Violence in Global Trade* (Minneapolis: University of Minnesota Press, 2014).

41 See Myriam Dunn Cavelty and Kristian Soby Kristensen, eds., *Securing "the Homeland": Critical Infrastructure, Risk, and (In)Security* (London and New York: Routledge, 2008).

42 Timothy Pettit, Joseph Fiksel, and Keely Croxton, "Ensuring Supply Chain Resilience: Development of a Conceptual Framework," *Journal of Business Logistics* 31, no. 1 (2010): 1–21; Cowen, *The Deadly Life of Logistics*; Collier and Lakoff, "Vital Systems Security."

https://doi.org/10.1017/cls.2019.5 Published online by Cambridge University Press

of vital points could continue under the *Emergencies Act* of 1988.[43] But in the late 1990s and early 2000s, a series of events forced a new understanding of vital systems that necessitated the invention of new strategies of governance, particularly the development of a security intelligence capacity for CI security. By 1996, an unresolved impasse over how to adapt the vital points program to the all-hazards orientation of the *Emergencies Act* effectively ended active work on the program that year.[44] At the same time, the federal government convened the National Contingency Planning Group (NCPG) within the Department of National Defence to assess the readiness of federal departments and major private-sector service providers (e.g., banks, telecoms, electricity providers) to respond to failures in their operations due to the Y2K changeover.[45] Instead of decomposing vital systems into discrete points to be measured, the NCPG adopted the language of "critical infrastructure"—which had recently been identified as a domestic security priority in the United States by the President's Commission on Critical Infrastructure Protection—and set out to gauge interdependencies between infrastructure sectors in order to assess major points of failure in the economic-political-social fabric of the country.[46] After the rollover, the NCPG was renamed the Critical Infrastructure Protection Taskforce (CIPTF), and shortly thereafter, it merged with EPC to form the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP). In the immediate wake of 9/11, the fledging OCIPEP attempted to revive the idea of a master list of CI in Canada, but concerns from industry about ownership and protection of proprietary and confidential data prevented further development of that approach.[47] Instead, OCIPEP built upon the approach pioneered through the experience of Y2K, which centered on creating partnerships with leading owner/operators amongst the six CI sectors it defined. This approach took embryonic form in OCIPEP's *National Critical Infrastructure Assurance Program* (NCIAP), which was further developed by OCIPEP's successor agency, Public Safety Canada, into the current *National Strategy for Critical Infrastructure*.

Space precludes a fuller analysis of the *National Strategy* in this article, but a crucial point to be made about this framework is that it does not derive from the exercise of exceptional emergency power, nor does it seek to install prophylactic enclosures around static objects of protection. Whereas the system of industrial security assembled during the Cold War flowed from the sovereign declaration of a national emergency (war or insurrection) to enable a particular style of temporally-limited governmental intervention (emergency protection), contemporary strategies for governing CI are underpinned by the epistemological understanding

43 David Peters, "Briefing Paper: The Vital Points Program," (2001). Unpublished memo obtained by email from author, April 8, 2016.
44 Ibid.
45 Interview with former NCPG staff analysts (2), September 14, 2015.
46 *Canada's Critical Infrastructure: An Overview* (Ottawa: National Contingency Planning Group, 1999).
47 *National Critical Infrastructure Assurance Program—Discussion Paper* (Ottawa: Office of Critical Infrastructure Protection and Emergency Preparedness, 2002).

of infrastructure disruptions as normal features of complex systems and aim instead to ward off or parry the potential for "self-amplifying irruptive disruption," in which minor disturbances cascade across interlinked systems to produce potentially catastrophic effects.[48] Moreover, and in contrast to the high modernism of the Cold War period in which vital points were discrete entities to be revealed with scientific accuracy, the "new" object of CI is understood to be dense, opaque, and possessing an independent reality accessible only through the pragmatic philosophy of "partnership" and "collaboration" structured around the often-cited statistic that 85% or more of CI systems are privately owned. With this new appreciation of the problem, our contemporary *dispositif* of infrastructure security draws on the "normal" powers and requirements of the *Emergency Preparedness Act* and its successor legislation, the 2007 *Emergency Management Act*, to foster and extend the logic of *resilience* on the part of self-governing owner/operators of CI facilities.[49] The production and distribution of security intelligence is a key mechanism within this *dispositif* of infrastructural resilience, one that functions to gauge risks incubating within the "fine materiality […] of exchange and circulation" so that infrastructure operators may modulate their systems in light of prevailing levels of risk in order to ensure continuity of services rather than react to emergency conditions with temporary protections. Below we sketch out the beginnings and ongoing development of this intelligence capacity within the RCMP and the changes it entails for the exercise of police power in regulating systems vulnerability in Canada.

Security Intelligence as Police Power

In the aftermath of 9/11, the RCMP faced numerous requests from across the federal government about the status of "vital points" in Canada, and the question of whether the program had been officially discontinued or was merely "stagnant" was actively discussed with the RCMP. In October 2001, a five-year, $500,000/year budget to revitalize the vital points program and bring it into line with the NCIAP was proposed, but by the end of the following year it was clear that the vital points program would not be integrated with the nascent NCIAP; instead, the NCIAP would displace the vital points program entirely. For the RCMP, this presented the necessity of "developing a position on this new initiative" that supported the "broad purpose, scope and mandate" of the NCIAP.[50] In this context, the RCMP established the basis for an in-house intelligence unit dedicated to CI security along the lines envisioned by Geddes and the McDonald Commission more than a decade prior and, in doing so, laid the foundation to rework the mechanisms through which police power is exercised.

---

48 Brian Massumi, "National Enterprise Emergency: Steps toward and Ecology of Powers," *Theory, Culture & Society* 26, no. 6 (2006): 153–85.

49 Boyle and Speed, "From Protection to Coordinated Preparedness; see also Philip J. Boyle, "'Building a Safe and Secure Canada: The Mechanopolitics of Infrastructure," *Resilience: International Policies, Practices, and Discourses* 7, no. 1 (2019): 59–83.

50 Emails pertaining to the Vital Points Program and National Critical Assurance Program, RCMP, October 2001–December 2002. AI-2016-03427.

https://doi.org/10.1017/cls.2019.5 Published online by Cambridge University Press

The development of an intelligence capacity for infrastructure security originates in the context of the broad push from the federal government to establish relationships with major infrastructure owner-operators in preparation for the Y2K changeover. In this context, the RCMP fashioned a role for itself as a producer and provider of information related to crime prevention and public safety amongst government and private-sector partners.[51] The success of the initiative—or lack of major failure attributable to Y2K—fit with the overall embrace of intelligence-led policing by the RCMP and led the force to seek a permanent intelligence unit dedicated to CI. After 9/11, funds made available through the federal Public Safety & Anti-Terrorism initiative allowed the RCMP to establish the Critical Infrastructure Criminal Intelligence section in January 2003.

Housed in the Federal Policing Criminal Operations Branch, the now-named National Critical Infrastructure Team (NCIT) functions as the hub of a network of intelligence production and exchange specific to threats to CI. Intelligence work is typically considered to be the preserve of the state, and of the "high policing" agencies of the state in particular, but the NCIT is an instance of new "hybrid" or "symbiotic" forms of intelligence work characterized by the integration of private sector security actors within police intelligence units and the two-way exchange of intelligence products.[52] The integration of corporate actors into the NCIT—and, conversely, the integration of the NCIT into the security operations of private corporations—occurs in multiple ways. One is the practice of seconding corporate security officials to work on-site with NCIT analysts for periods of up to a year. In July 2015, the NCIT had two private sector secondments embedded within the NCIT.[53] A second and more longstanding mechanism for brokering CI security intelligence is the NCITs Suspicious Incident Reporting System (SIR), an online information platform developed under the auspices of the federal government's Rail and Urban Security Initiative in 2008. The SIR enables private sector subscribers—typically a senior security staff member or delegate(s) with Level 2 (Secret) security clearance—to report suspicious incidents directly to the NCIT using what are known as Suspicious Incident Reports. In some cases, the NCIT may refer suspicious reports to the police of the jurisdiction for investigation. Analysts in the NCIT also collate anonymized reports with other classified or open sources of information to produce topic- or sector-based assessments that are distributed back to private-sector subscribers as various intelligence products or used in briefings provided by NCIT staff to public or private sector audiences. In July 2015, 140 private companies had full access to submit and receive information through the SIR with an additional

51 Interview with Officer in Charge (1) & staff (5), National Critical Infrastructure Intelligence Team, Royal Canadian Mounted Police. July 8, 2015.

52 See Jean-Paul Brodeur, "High Policing and Low Policing: Remarks about the Policing of Political Activities," *Social Problems* 30, no. 5 (1983): 507–20; Peter Gill and Mark Phythian, *Intelligence in an Insecure World*, 2nd ed. (Cambridge, UK: Polity Press, 2012); Conor O'Reilly and Graham Ellison, "'Eye Spy Private High': Reconceptualizing High Policing Theory," *British Journal of Criminology* 46, no. 4 (2005): 641–60.

53 Interview with Officer in Charge (1) & staff (5), National Critical Infrastructure Intelligence Team, Royal Canadian Mounted Police. July 8, 2015.

https://doi.org/10.1017/cls.2019.5 Published online by Cambridge University Press

seventy approved to submit Suspicious Incident Reports only.[54] Collaborations may also be incident/issue specific. For example, in 2010, NCIT and several RCMP divisions worked directly with CSIS and Enbridge security to formulate "an integrated intelligence production plan" regarding opposition to the company's proposed Northern Gateway pipeline. This plan was to develop "an initial intelligence product that [could] be expanded upon as the Pipeline moves along in its various stages of development."[55] Further, the RCMP also participates in sector-specific network meetings that bring together government officials, owner-operators and other industry stakeholders to discuss matters related to CI.[56]

The NCIT thus engages in a form of intelligence activity that can be understood as "game management" or "intelligence brokerage" that operates by "bringing together otherwise disparate actors, problems and solutions."[57] Since 2004, this hybrid intelligence node has been integrated into a wider restructuring of national security responsibilities under the federal National Security Policy (NSP). The NSP fuses the work of national security, law enforcement, and emergency management under the purview of Public Safety Canada and prioritizes enhancing federal intelligence capabilities as part of developing an "integrated security system" for Canada's contemporary security needs. The delegation of emergency management responsibilities to all federal government departments and agencies horizontalizes and expands the security intelligence form of police power. The NSP specifies CI as an object of national security and disruptions to CI as a national security offence, thus integrating these government departments and agencies—which do not have official law enforcement or "security-intelligence" mandates—as essential to auditing and risk-assessing CI. Rather than diluting state power, this reorganization of national security to expand responsibilities for CI risk management across government and the private sector is concomitant with the centralization of authority via the *strategic* role carved out by Public Safety Canada and its enforcement agencies, particularly the RCMP. As noted in an NCIT email, the private energy sector "does not have ready access to criminal intelligence that will identify potential and/or credible criminal threats," making it "incumbent upon the appropriate federal and provincial authorities to share responsibility for the protection of Canada's energy sector."[58] As part of the aim of creating an overall intelligence picture amongst stakeholders on threats to national security, Suspicious Incidents Reports submitted to the NCIT are made available in raw form to CSIS as well as shared with Integrated National Security Enforcement Teams (INSET) when necessary.

Importantly, legislative changes brought in support of the NSP in the 2007 *Emergency Management Act* (EMA) also sought to address the reluctance of

---

54 Email Communication, Officer in Command, National Critical Infrastructure Team, July 10, 2015.

55 RCMP National Security Criminal Investigations, "Enbridge Northern Gateway Pipeline Project—Intelligence Production Meeting," (2010), and "Aug 6th Northern Gateway Project" [Email] (2010). AI-2017-04539.

56 Pasternak and Dafnos, "How Does a Settler State...?"

57 Gill and Pythian, *Intelligence in an Insecure World*, 73.

58 RCMP National Security Criminal Investigations, [Email] (January 12, 2012). AI-2017-04539.

https://doi.org/10.1017/cls.2019.5 Published online by Cambridge University Press

private industry to share information with the NCIT and its partners—due to potential risks of legal and regulatory actions by revealing negligence or vulnerabilities, sharing proprietary information with competitors, or negative impacts on consumer and shareholder confidence—by exempting CI-related information from the release requirements of the *Access to Information Act*. Under this exemption, the RCMP or any other federal actor may refuse disclosure of "third party information" relating to "the vulnerability of the third party's buildings or other structures, its networks or systems, including its computer or communications networks or systems, or the methods used to protect any of those buildings, structures, networks or systems." This legal mechanism for secrecy, coupled with the proliferation of formal (e.g., SIR) and informal nodes and circuits of information and intelligence exchange, is aimed at assuring industry partners that information sharing "is not intended to be used to penalize participants."[59] These circuits of security intelligence forged by and in secrecy are quickly becoming "infrastructural" to the very processes of accumulation they secure and continue to proliferate through an expanding understanding of "risk" underlying the problem-space of systems vulnerability.

Security Intelligence as Pacification

The formation of the new and expanding security intelligence networks we have described above is an expression of a deeper ambition to mobilize "risk" as strategy in the governance of systems vulnerability. The idea of "risk" played only a marginal role in the vital points program. Indeed, insofar as risk denotes not only a way of thinking about the future but also a set of mechanisms for calculating it, there was no appreciation of "risk" in governance of vital points at all. Instead, plans to protect vital points derived from the 30,000-foot view of military expectations of the form and scale of future war updated over periods of up to a decade. Today, security intelligence is a foundational mechanism with which the "fine materiality of exchange and circulation" is sifted and sorted, with undesirable elements made amenable to intervention. But the operative form of "risk" at play in this context departs from the calculative practices of insurance valorized as the archetype of risk thinking. Security intelligence, as Gill and Phythian, define it, is inherently about "providing forewarning of threats or potential threats," yet intelligence work is not necessarily, nor even primarily, a calculative practice.[60] Rather, the work of security intelligence is often "prognostic and strategic" in nature, with considerable room for speculation, conjecture, and plain guess-work to exist alongside probabilistic ways of thinking about the future.[61]

[59] Public Safety Canada, "Critical Infrastructure Information Sharing Framework," (n.d.): 6. A-2015-00258.

[60] Gill and Pythian, *Intelligence in an Insecure World*, 19.

[61] Steven Hutchinson, "Intelligence, Reason of State and the Art of Governing Risk and Opportunity in Early Modern Europe," *Economy and Society* 43, no. 3 (2014): 370–400; see also Philip Bougen, "Catastrophe Risk," *Economy and Society* 32, no. 2 (2003): 253–74; Stephen Collier, "Enacting Catastrophe: Preparedness, Insurance, Budgetary Rationalization," *Economy and Society* 37, no. 2 (2008): 224–50.

Since 9/11, the logics of biopolitical and geopolitical security have tended towards contemplating remote but potentially catastrophic risks rather than those that are merely probable.[62] There is, of course, a longer genealogy of this way of thinking having to do with the threat of nuclear war, though the density and complexity of contemporary vital systems security are seen to harbour the potential for even small-scale disruptions to cascade across multiple systems, and perhaps all systems, with catastrophic effects. A post-9/11 threat analysis conducted by OCIPEP, for example, identifies the need to encourage "robust and flexible mitigation preparedness, and response and recovery plans" amongst public and private operators of CI because of the possibility, "*regardless of how remote* that an event on an equally grand scale might occur again" (emphasis added).[63] In turn, the embrace of worst-case thinking in the governance of CI is driving the expansion of the definitions, nodes, connections, flows, and scope of the security intelligence apparatus we have described above. Importantly, the form and content of this intelligence work is also being shaped by the securitizing moves of private industry to define what "counts" as CI and the sources of disruption to CI networks. The relay of Suspicious Incident Reports, for example, is not simply a technical way of conveying information. They are also performative speech acts that configure the materiality of CI by making claims for some circulatory elements and systems to be recognized as more important than others and thus in need of specialized care.[64] Paralleling this is the discursive work of "threat entrepreneurs," such as senior intelligence officials, corporate security officials, or risk and insurance industry representatives, who circulate between public and private spheres and construct broadly shared understandings of the multiplicity of "non-traditional" threats facing CI today.[65]

The definition of a "vital point" derived from the needs of war, but over the last two decades, the confluence of worst-case thinking and the definitional work of private sector "partners" in CI security are shaping the elastic notion of CI around the material instruments and impetuses of capital accumulation. Both understandings of vital systems are biopolitical in the sense that war and capital accumulation are closely-linked activities that can be undertaken or justified in terms of the well-being of a population. The shift in governmental strategies we have examined are thus not a matter of CI security "becoming biopolitical" at some recent point in time. Instead, this shift is significant for the different sources of biopolitical danger they diagnose. If the framing of vital points as a problem of waging industrial war necessitated the invention of a system for "differentiating inside a territory between what is important and what is not" in order to protect those elements from external enemies thought to have *infiltrated* the population,

---

62 Louise Amoore, "Security and the Incalculable," *Security Dialogue* 45, no. 5 (2014): 423–39; Philip J. Boyle and Kevin D. Haggerty, "Planning for the Worst: Risk, Uncertainty, and the Olympic Games," *The British Journal of Sociology* 63, no. 2 (2012): 241–59.

63 Government of Canada, *Threats to Canada's Critical Infrastructure* (Ottawa: Office of Critical Infrastructure Protection and Emergency Preparedness, 2003).

64 Claudia Aradau, "Security That Matters: Critical Infrastructure and Objects of Protection," *Security Dialogue* 41, no. 5 (2010): 491–514.

65 Monaghan and Walby, "Surveillance and Environmental Movements."

https://doi.org/10.1017/cls.2019.5 Published online by Cambridge University Press

the reframing of CI as the foundations of our (liberal) way of life has given rise to a security regime that targets the population *itself* for harbouring sources of malicious disruption to CI.[66] Contemporary strategies of infrastructure security are of course attuned to non-malicious sources of disruptions—weather, industrial accidents, and so on—but the extent to which elements of the population itself present threats to CI demands strategies of pacification ranging from passive monitoring of "suspect" or "threatening" populations to coercive, pre-emptive force to suppress the disruptive potential they hold for the logistical efficiency of the contemporary economic and political order.

This pacification work is most visible in relation to Indigenous peoples' assertions of jurisdiction, particularly in the context of resource extraction in Canada. The emergence of CI as the object of national security and Canada's economic prioritization of increasing extractive industries creates a context in which Indigenous self-determination and environmentalism have become sources of national security concern. Within our contemporary *dispositif* of infrastructure resilience, Indigenous communities, groups, and individuals are construed as national security concerns in this context in two ways: first, where physical CI is located on or near First Nations, Inuit, or Métis communities, and second, when assertion of their rights and jurisdiction creates uncertainties for governments and corporations, thus jeopardizing current and possible future bases of accumulation. In 2007, the RCMP formed an Aboriginal Joint Intelligence Group (JIG) to gather information and "produce and disseminate intelligence concerning conflict and issues associated with Aboriginal communities."[67] External contributors to, and recipients of, the JIG's intelligence included CSIS, other government departments and law enforcement agencies, and energy sector partners. One key area of concern for the JIG was "tension against critical infrastructure" stemming from blockades and impacts on "energy sector development."[68] Although officially disbanded in November 2009, the JIG's security intelligence work in relation to CI and Indigenous communities has been diffused through the channels anchored by the NCIT.[69] Whether through legal challenges or direct actions such as blockades, Indigenous peoples' exercises of jurisdiction can directly and indirectly disrupt existing circulations through these infrastructures and prospects for future projects.[70]

The surveillance of Indigenous peoples and political movements is nothing new; what is distinct is how it expands substantively and temporally in ways that are legitimated by the primary objective of eliminating obstacles to accumulation to open up and expand the desirable circulations of supply chains. As an NCIT intelligence assessment distributed to industry partners notes, "it is often difficult to justify in the court of public opinion, conducting criminal investigations associated to the noble

66 Didier Bigo, "Protection: Security, Territory, and Population," in *The Politics of Protection. Sites of Insecurity and Political Agency*, ed. Jef Huysmans, Andrew Dobson, and Raia Prokhovnik (London and New York: Routledge, 2006), 84–100.
67 RCMP, "RCMP Criminal Intelligence. Aboriginal Joint Intelligence Group. Aboriginal Communities, Issues, Events and Concerns 2009/10" (2009): 5. A-2011-06291.
68 RCMP, "NAPS 2009 POWPM", [deck] (2009): 2. GA-3951-3-03434/11.
69 Dafnos et al., "Surveillance and the Colonial Dream."
70 Pasternak and Dafnos, "How Does a Settler State?"

https://doi.org/10.1017/cls.2019.5 Published online by Cambridge University Press

cause of protecting the global environment."[71] The centering of CI disruption as a matter of national security provides a justification. Similarly, while intelligence reports frequently note the historical lack of violence or criminal offences in Indigenous peoples' protests, the enduring *potential* for infrastructure disruption provides the rationale for extensive monitoring of Indigenous movements by a complex of government departments—including, notably, Indigenous Affairs and Northern Development Canada—as part of their CI and emergency management responsibilities.[72] The NCIT plays a crucial role in this surveillance, whether in relation to Indigenous self-determination or other "suspect" populations, by cataloguing the activities of "Aboriginal extremists," "non-violent criminal activists,"[73] suspected Jihadists, eco-terrorist groups, as well as typologies of advances in "extremist tradecraft" (such as using drones or Google Earth for aerial surveillance of targets) in the intelligence products it circulates to its public and private clients to inform the security plans of owner/operators or coercive intervention by other state actors. In these products, we can see that the seemingly archaic strategy of list-making that is quintessential of police power is not displaced by contemporary strategies of infrastructure preparedness but reconstituted within the RCMP's intelligence apparatus as a mechanism for sifting amongst circulations that are to be valued for collective life and indexing those that pose a threat to the "normal worlds of transnational capitalism" in the pacification project that is CI security.[74]

Conclusion

In this article, we have examined the historical conditions of how security intelligence came to be embraced as a logistical strategy for governing the problem of systems vulnerability in Canada. As we have shown, the system of emergency powers in place in Canada in the middle of the twentieth century enabled the governance of systems vulnerability to take a particular form during the Cold War that was concerned mainly with developing localized archipelagos of physical protection to be implemented during war. Amid the exponentially expanding infrastructural milieu and accelerated by the logistical and digital revolutions and the repeal of the WMA in 1988, critical infrastructure was constituted in the 1990s as a "new" security object of concern to be governed without explicit recourse to exceptional sovereign power. In this context, the RCMP fashioned a new role for itself as a broker of security intelligence about threats to infrastructure systems "incubating within the present" rather than inspector and advisor of specific security arrangements.[75]

---

71 RCMP National Security Criminal Investigations, "Environmental Criminal Extremism and Canada's Energy Sector" (2011): 8. A-2013-01509.

72 Dafnos et al., "Surveillance and the Colonial Dream"; Dafnos, "Pacification of Indigenous Struggles in Canada"; Tia Dafnos, "The Enduring Settler-Colonial Emergency: Indian Affairs and Contemporary Emergency Management in Canada," *Settler Colonial Studies* (2018) DOI: 10.1080/2201473X.2018.1491157.

73 RCMP National Security Criminal Investigations, "Environmental Criminal Extremism and Canada's Energy Sector" (2011): 8. A-2013-01509.

74 Allen Feldman, "Securocratic Wars of Public Safety," *Interventions* 6, no. 3 (2004): 330–350.

75 Ben Anderson, "Preemption, Precaution, Preparedness: Anticipatory Action and Future Geographies," *Progress in Human Geography* 34, no. 6 (2010): 777–98.

https://doi.org/10.1017/cls.2019.5 Published online by Cambridge University Press

In our view, these changes are significant not because they point to a historic form of scope creep in which old and new threats are now conjoined. Instead, the formation and ongoing expansion of the public-private intelligence networks we have described above is best understood as a recent modulation in the longstanding exercise of police power—understood as the power to enact a particular ordering of the material foundations of industrial and economic circulation. Today police power no longer operates by taxonomizing vulnerabilities in the industrial milieu to be secured but through the production and exchange of security intelligence amongst overlapping fields of public and private security actors who co-construct the materiality of CI *and* the sources of infrastructural disruption seen to lurk within contemporary biopolitical existence. This is a recent shift of modality in the exercise of police power, one that occurred in response to a new appreciation of systems vulnerability that came into view in the late 1990s. Critically, this modality does not flow from exceptional sovereign prerogative but is accomplished in ways that are routine, ongoing, and derive from regular powers of government. And as we have pointed out, the critical consequence of the normalization of police power (in the form of security intelligence) is that it enables the extension of hybridized or symbiotic forms of surveillance of the population on the basis of the threats to CI harboured therein, thus giving rise to a regime of infrastructure security privileging the security of technical systems over the biopolitical interests of elements of the population they are intended to support.[76] In this regime, for example, the potential disruptiveness of Indigenous self-determination or environmentalism are treated as malicious threats to be pre-emptively suppressed or part of the assortment of "natural givens" to be folded into the normal course of operations alongside the portfolio of "natural" risks facing energy infrastructure projects (storms, floods, accidents, etc.). Clearly, then, much more work can be done towards understanding the biopolitical dimensions of the evolving regime of infrastructure security as new or modified tactics are deployed in the name of securing conditions for "optimized" circulations of liberal capitalist colonial order.[77]

Philip Boyle
Sociology & Legal Studies
University of Waterloo, Waterloo, Ontario
pjboyle@uwaterloo.ca

Tia Dafnos
Department of Sociology
University of New Brunswick, Fredericton
tdafnos@unb.ca

[76] Julian Reid, "Conclusion: The Biopolitics of Critical Infrastructure Protection," in Dunn Cavelty and Kristensen, *Securing "the Homeland"*, 76.

[77] For a very recent analysis of these issues, see Miles Howe and Jeffrey Monaghan, "Strategic Incapacitation of Indigenous Dissent: Crowd Theories, Risk Management, and Settler Colonial Policing," *Canadian Journal of Sociology* 43, no. 4 (2018): 325.

https://doi.org/10.1017/cls.2019.5 Published online by Cambridge University Press