TSAS

canadian network for research on terrorism, security and society

Working Paper Series

No. 14-05

June 2014

The Effectiveness & Effects of Canada's Integrated National Security Enforcement Teams

Veronica Kitchen

The Canadian Network for Research on Terrorism, Security, and Society

TSAS is supported as a national strategic initiative funded by **SSHRC** and **Public Safety Canada**, along with the following departments of the federal government:

- Canadian Security Intelligence Service (CSIS)
- Citizenship and Immigration Canada (CIC)
- Royal Canadian Mounted Police (RCMP)

TSAS also receives financial support from the University of British Columbia, Simon Fraser University, and the University of Waterloo.

 For more information, contact the Co-directors of the Centre, Daniel Hiebert, Department of Geography, UBC (daniel.hiebert@ubc.ca) and Lorne Dawson, Department of Sociology and Legal Studies, University of Waterloo (ldawson@uwaterloo.ca).

Table of Contents

What do we mean by effectiveness? 1

Limits of cost-benefit analysis 4

Effects not just Effectiveness 5

The Politics of Security 8

Challenges of Security Research 9

The Integrated Model and the Evolution of Canada's INSETs 10

Trends in National Security Policing 13

- i. Formalization 13
- ii. Co-ordination 14
- iii. Information gathering and sharing 15

Conclusion 16

References 17

TSAS

canadian network for research on
terrorism, security and society

Working Paper Series

The Effectiveness & Effects of Canada's Integrated National Security Enforcement Teams

Veronica Kitchen

Department of Political Science, University of Waterloo

Canada's Integrated National Security Enforcement Teams (INSET), operated by the RCMP, have been an integral part of Canada's post-9/11 counter-terrorism apparatus for a little over a decade. As with analogous institutions in other countries, the goal of the INSETs was to counter the problem of 9/11, diagnosed as a failure to connect the dots, by bringing together all relevant stakeholders into common institutions. This paper is a first step in studying their emergence and evolution. First, I review the existing literature on evaluating counter-terrorism, and outline a number of concerns with existing methods. I argue that evaluating the INSETs requires taking three things seriously: first, the limits of the rational model of cost-benefit analysis; second, the politics of security; and third, the difficulties of doing security research. Next, I review the history of the INSETs in the context of the RCMP's national security program, noting key points of change. Finally, I briefly discuss how the model of integration exemplified by the INSETs influence *efficiency* (the use of resources), *effectiveness* (how well the institution works relative to its stated goals), and *effects* (the impact of policies on politics and society). The results are preliminary and are part of a larger, comparative project (Kitchen and Molnar n.d.; Kitchen forthcoming; Kitchen and Rygiel n.d.; Dunton and Kitchen 2014).

What do we mean by effectiveness?

What does it mean for a counter-terrorism policy or institution to be effective? There are several conceptualizations extant in the literature. Most focus on outcomes. The most high-profile effort to evaluate counter-terrorism policies is probably Mueller and Stewart's *Terror, Security and Money: Balancing the Risks, Benefits and Costs of Homeland Security* (Mueller and Stewart 2011). This book uses what it calls "standard risk and cost-benefit evaluation techniques that have been accepted and used throughout the world for decades by regulators, academics, businesses, and governments" to conclude that terrorism is a low-risk hazard to which massively excessive expenditures have been applied (Mueller and Stewart 2011, 172). Like other scholars, Mueller and Stewart's approach is outcome-based: they calculate loss, risk, and benefits in terms of the probability of a successful attack and the losses sustained in the successful attack (Mueller and Stewart 2011, 25). They highlight the opportunity costs of such overspending, but lament that Washing-

ton's homeland security bureaucracy has become a "self-licking ice-cream cone" that is likely to persist, despite the best evidence that it should not (Mueller and Stewart 2011, 185). So, effective counter-terrorism is terrorism that reduces terrorist attacks. Lum, Kennedy, and Sherley (2006) measure effectiveness similarly: do the measures reduce the likelihood of or damage from a terrorist attack, or do they discourage individuals from committing such attacks? Van Um and Pisoiu (2011) discuss effectiveness in a slightly more sophisticated way. They seek to measure: output effectiveness (whether policies, regulations, or other mechanisms have been implemented), outcome effectiveness (the measurable effects of policies--do they have the intended outcome?), and impact effectiveness (does it reduce terrorism?) (van Um and Pisoiu 2011, 3). They illustrate the differences between these three facets of effectiveness through the example of targeting terrorist financing: output effectiveness would measure the implementation of regulations related to terrorist financing, outcome effectiveness would measure the number of assets frozen or the effects on the financing of terrorist groups, and the impact effectiveness would measure the resulting level of terrorism (van Um and Pisoiu 2011, 4). Each of these perspectives assumes that we can measure counter-terrorism in terms of efficiency (how much benefit we get from a particular cost) and outcomes. Other studies look more clearly at effects on society (Crenshaw 2010); here, the critical literature has been more prevalent. As I will demonstrate, there are a number of problems with evaluating effectiveness in terms of outcomes. Some of these are inherent to the domain of counter-terrorism, and others are inherent in the positivist, rationalist methods used by most scholars to evaluate counter-terrorism.

Counter-terrorism institutions are complex concatenations of actors, policies, formal and informal organizations that cross the boundary between the domestic and the international as well as the boundary between the public and the private. Evaluating them as institutions necessarily requires drawing boundaries where evaluation will begin and end: it seems unlikely that a single study will be able to evaluate all the actors connected with a single institution. Moreover, it is not always clear what should be analysed. Even restricting the set to institutional effectiveness, one must ask whether security institutions should be analysed on the basis of what they are supposed to be doing (according to legislation and other guiding documents) or what they

are actually doing (Gerspacher and Dupont 2007)"plainCitation":"(Gerspacher and Dupont 2007. The field of counter-terrorism is characterized by mandate expansion and mission-creep. For instance, while fusion centers in the United States are supposed to have a mandate for data analysis and dissemination activities (Department of Homeland Security 2012), there is evidence that many fusion centers are engaged not just in data analysis activities but also data collection activities such as monitoring websites or processing footage from law-enforcement cameras, and also that they store data as well (Citron and Pasquale 2011, 1451–1452). In Canada we have seen the creation of new categories of threat, notably "multi-issue extremists" (Monaghan and Walby 2012).

Even if an analyst makes a decision to focus on one or the other, there is still the matter of working out what the goals of a particular institution are. These are not always well defined, or articulated in terms of what an organization should do rather than why it should do it (Department of Homeland Security 2010). While this may make evaluating success in terms of expectations straightforward, it makes it more difficult to evaluate outcomes. Furthermore, different parts of an organization may have overlapping goals. While this is a problem for institutions from the perspective of being inefficient (Jiao and Rhea 2007, 393), it is also a problem from the perspective of measuring effectiveness. In some cases, mandates may well be contradictory. The goals of effectiveness and accountability may also be in tension, and the creation of new networks sometimes favours effectiveness over accountability (Gill 2009). Similarly, political goals must be balanced with efficiency goals. There is some evidence that the tendency to gather more and more information for fear of missing something may be problematic not only from a privacy perspective, but also from an efficiency perspective: more information might actually make it more difficult to find the piece of information you want (the needle-in-a-haystack problem). Finally, some goals may have a very long timeline. In the case of preventing terrorist attacks through preventing radicalization or fostering resilience, the timeline may be measured in decades or generations. How do you measure effectiveness along the way? (Pantucci 2010).

Evaluating counter-terrorism institutions from a critical perspective exposes a key problem with the efficiency- and outcomes-based perspectives described above. Most obviously, trying

to measure success of the goal of preventing terrorist attacks quickly becomes ridiculous, particularly to those without access to detailed intelligence information because they are forced to distinguish between terrorist attacks that did not happen because of preventive measures, and terrorist attacks that did not happen because they were not going to happen anyhow. Deterrence may be effective, but it is hard to measure from any perspective. Moreover, terrorist goals and counter-terrorist institutional goals may be at odds: if it is a goal of terrorist groups to generate overspending by governments' counter-terrorism programs, then they may achieve their goal at the same time as policy makers achieve theirs–reducing terrorist attacks (Perl 2007). The most important challenges to the measurement of effectiveness, however, are rooted in the differences between critical and rationalist methods. These are the failure of rational calculus, the exceptional nature of security, the need to evaluate effects as well as effectiveness, and the difficulties of doing security research.

Limits of cost-benefit analysis

Rationalist studies of counter-terrorism use a standard cost-benefit analysis, asking, broadly, whether any given policy, practice, or institution has made society safer. Such arguments are based on the idea that it is possible to make calculations about tactics, risk, and probability. However, the difficulty with this perspective is that terrorism is a low-probability event, so there are mercifully few cases to analyse. Moreover, it is almost impossible to isolate the results of any particular policy as instrumental in reducing terrorism or deterring a specific attack. There are also important constitutive effects that are not adequately captured in a rationalist approach. Finally, we cannot know if non-attacks are caused by government actions or some other factor.

Terrorism is a low-probability, high-risk event. Models such as that of Mueller and Stewart (2011), which focus on the probability of an attack, break down under such circumstances. Ulrich Beck (2006) argues that rationality "encourages the anticipation of the wrong kind of risk, the kind we can calculate and control, whereas disaster arises from what we do not know and cannot calculate" (330). Thus while democratic governments may curtail civil liberties in an attempt to provide security, such efforts are doomed to be ineffective (330). This should suggest to us that rational calculations of cost-benefit analysis are not necessarily a good way to analyse effective-

ness. In contrast to Beck, Aradau and van Munster (2007) argue that we have to take into account the fact that risks are socially constructed. They are not objectively "out there" to be known or not known, as Beck argues. Rather, we render them calculable and knowable by the ways we think about them (Aradau and Van Munster 2007, 96). For instance, migrants are sometimes constructed as a security threat although there seems to be little objective evidence that they are any more likely to be a threat than others in the population (Huysmans 2006). Aradau and van Munster (2007) argue that when faced with the possibility (and unknowability) of a catastrophic future and the uncertainty of whether it will come to pass, governments turn to precaution as a way of governing the future (100). Governments employ the technologies of attempting to maintain zero risk, basing projections on worst-case scenarios that expect irreversible damage, and shifting the burden of proof to citizens, not intelligence officials (Aradau and Van Munster 2007, 103). Under conditions of uncertainty–where we can't know what a terrorist attack will look like, when it will come, or who will perpetrate it–this has the effect of making surveillance and control mechanisms that act on the whole population more desirable (Aradau and Van Munster 2007, 104). Given the limits of intelligence and surveillance tools, a decision about who (or what) is a threat becomes an administrative decision based on the goal of maintaining zero risk, rather than a decision based careful weighing of the evidence (Aradau and Van Munster 2007, 106). In the counter-terrorism context such administrative decisions manifest in subjecting people to sanctions based on "pre-crime" or "pre-terrorism", which I discuss below. This failure of rationality provides a (partial) explanation for the overspending identified by Mueller and Stewart (2011), but also an argument for why the rational-analytic method will not provide a complete picture of effectiveness. But what does the failure of rational calculus mean for how we should evaluate effectiveness? Evaluating effectiveness will be more about identifying conditions of possibility that enable certain kinds of politics and practices but close off others.

Effects not just Effectiveness

Perhaps the most important insight critical security scholarship brings to a discussion of evaluating effectiveness is that one cannot simply study efficiency, one must also study effects. Measuring efficiency with respect to outcomes is, as I have already discussed, impossible from a

critical perspective. It may be possible to measure efficiency at a more micro-level, as suggested by van Dongen (2011). He argues that "rather than identifying metric measures of success for a counter-terrorism policy as a whole and looking for combinations of measures whose introduction is followed by desirable scores, such as lower numbers of terrorist attacks" (358), one should be "breaking up success in counter-terrorism into several separate components, the strategic-level pillars of a counter-terrorism policy" (358). He argues for identifying the causal chains through which any policy or part of a policy is supposed to lead to a given outcome. Evaluating effectiveness, then, is a matter of seeing whether or not the causal chain unfolds in reality in the way that it was designed to do (van Dongen 2011, 367). This makes sense if we think about causality in terms of conditions of possibility: does the policy create the conditions of possibility for particular outcomes that it was designed to create? (see also Lindekilde 2012, 339).

However, this method may still lead to what I call the checklist problem: managerial methods of measuring effectiveness–that is, measuring effectiveness in terms of metrics that compare actions to a pre-defined list of criteria–may have the effect of hiding policies or practices from the public eye. Checklists may create the impression that policies or procedures are apolitical, when security is always political. For instance, the US Department of Homeland Security's Baseline Capabilities for State and Major Urban Area Fusion Centers is presented as a checklist of capabilities and capacities that fusion centers must achieve in order to have the "necessary structures, processes, and tools in place to support the gathering, processing, analysis and dissemination of terrorism, homeland security, and law enforcement information" (Department of Homeland Security 2010, 1). Each capability is described briefly in technocratic language. Several, however, disguise fundamentally political and contested ideas. "Capability D4", for instance, states that "fusion centers shall ensure that analysts are able to understand and identify the links between terrorism-related intelligence and information related to traditional criminal activity so that they can identify activities that are indicative of pre-cursor behaviours, terrorist activities, and threats" (Department of Homeland Security 2010, 19). This capability pre-supposes that such links exist, and that understanding them is a good way to prevent terrorism. It also creates the conditions for policies of surveillance and reactions of suspicion from targeted individuals and

communities.

Solving the checklist problem means being conscious of the political context behind managerial decisions. Lindekilde (2012) notes that the securitizing move described above is important not simply because it elevates a matter beyond normal politics and thus beyond normal measures of efficiency. The timing and context of the securitizing move that elevates something into a threat may influence the way policy is designed and implemented. The discursive presentation of a threat prior to policy formulation may affect the way it is formulated, and may continue to influence the way it is presented. Lindekilde offers the example of counter-radicalization, where discourses that stigmatize particular communities may render particular policies less effective or even counter-productive (Lindekilde 2012, 339). The way we talk about policy influences how well policy works. So, we must not simply consider effects, but also how effects affect effectiveness.

A critical perspective on measuring terrorism effectiveness must be able to evaluate not simply whether particular policies lead to the outcomes they were designed to and the political context of the implementation of policy, but also the effects of particular policies. This is imperative because of the reflexivity inherent in a critical method: just as we cannot know the world except as it is filtered through the way we think and talk about the world, the way we talk about the world influences the way the world is. Therefore, short-term and long-term societal effects must be integrated into our understanding of effectiveness. Two examples make the point here. First, most arguments about counter-terrorism talk about trade-offs between security and liberty with the goal of policy to achieve the correct balance between security and liberty. However, some critical scholars have begun to make the argument that the relationship between these two ideas is not one of trade-off. Security measures are not eroding *or* protecting civil liberties. Rather, security measures reshape the meaning of liberty and freedom. Security is a mode of governing freedom (Neocleous 2008; Bell 2011). For instance, Colleen Bell (2011) argues that the creation of the National Security Roundtable in Canada is a mechanism through which the Canadian government has shifted responsibility for identifying and addressing potential terrorists to particular ethnic groups rather than conceptualizing it as a problem for all Canadians. A second example

is the example of pre-crime. In the context of high-consequence, low-probability events and the failure of rationality described above, the way we think about terrorism and terrorists changes as well. McCulloch and Pickering (2009) argue that under such circumstances, the concept of prevention is equated with "pre-crime". Prevention becomes a task of identifying people who might become terrorists, rather than identifying the root causes of terrorism (McCulloch and Pickering 2009, 629). Thus terrorism becomes a "status offence" that targets individuals because of who they know rather than what they have done (633). So, evaluating effectiveness must take into account such societal effects beyond balancing liberty and security, or efficiency and ethics.

The Politics of Security

The politics of security also make it difficult to evaluate security institutions. Claims to security are used to legitimate certain kinds of politics. According to the Copenhagen school, security is a speech act that elevates an issue beyond normal politics, justifying the use of extraordinary measures (Buzan, Waever, and De Wilde 1997). Therefore, it also elevates it beyond normal measures of efficiency, accountability, and effectiveness (see Kitchen and Rygiel n.d. on accountability). Security is used as a legitimizing discourse to undertake particular practices that would not otherwise be permitted. For instance, during the G20, the Toronto Police promulgated–and allowed the media to promulgate–a misunderstood interpretation of an obscure regulation of the Ontario Government that led to a public belief that stop-and-searches being conducted all over town by police officers were legitimized in the name of security. This presents at least two problems for measuring effectiveness. First, it makes measures of efficiency almost meaningless. Even in a rational calculation, it is, ultimately, a value judgment whether spending an extra dollar on security measures is worth the marginal increase in safety it provides. Therefore (and second), we cannot understand effectiveness without understanding the politics of security. Effectiveness is really only comprehensible in the context of a particular time, place, and set of norms and values.

Challenges of Security Research

The ability of an outside researcher to evaluate security institutions is rendered more difficult by the secrecy of security institutions as well as by the subject-position of the researcher. The research approval process for most security institutions in Canada is long and access to security officials is always limited. For instance, I embarked on this study hoping to study socialization within new security institutions. I wanted to interview RCMP and other officers seconded to the INSETs as a way of understanding the micro-politics of integration. Unfortunately, I was not allowed to interview such officers, which severely limited what I could say about an important research question. Research on security in Canada is likely to become more difficult. Recently, the federal government amended a schedule to the Security Information Act such that it permanently binds current and former employees of most of the government divisions concerned with Canada's national security–including the RCMP's National Security Program–from releasing "special operational information", even long after they have retired (Boutilier 2014; P. W. and G. S. C. Government of Canada 2014). Similarly, the Privacy Commissioner reported in August 2013 that the RCMP had not responded to an Access to Information Provision request in several months (Minsky 2013). While the RCMP has now resumed responding to ATIP requests and posting them on its website, it ought not to have taken being called-out by the Privacy Commissioner for the RCMP to fulfill its legal duty. Such difficulties in doing security research are to be expected. This is, after all, an operationally sensitive area. But it does mean that researchers are constrained in what they can say and how they can do research. Any evaluation of Canadian security policies and institutions is always partial.

Security research is also shaped by the subjectivity of the researcher. The researcher's subject position in relation to that which she or he is studying will influence the way she or he is able to measure effectiveness. Gender, age, race, experience with terrorism, experience with bureaucratic institutions, and the relationship between the researcher and her or his research subjects will all influence the way the researcher conceives of effectiveness. Someone junior (and female) may either be perceived as unthreatening and may induce interview subjects to speak more freely,

or she may be perceived as incompetent and receive the same, basic speech that rehashes what is available on the website over and over again. A researcher who has spent years developing relationships with security officials may be trusted with more interesting information or more candid remarks, but may also, therefore, find it more difficult to speak critically about his or her friends or colleagues. This subjectivity is inevitable. It is impossible to erase bias. The solution is therefore not to try to create an illusion of objectivity, but rather to be transparent about the bias, other kinds of subjectivity, and the ways it influences the research.

The Integrated Model and the Evolution of Canada's INSETs

The idea of putting policing officials with different expertise together in the same operational unit pre-dates 9/11 and has antecedents outside of counter-terrorism. Faced with a threat from the FLQ in the 1960s, the RCMP, Sûreté de Québec, and Montreal Police co-operated in a task force to respond to the situation and disbanded after the October Crisis in 1970 (Schneider and Hurst 2008, 362). The idea also has antecedents in integrated homicide squads, and in Canada integrated teams were used during the 1990s in the so-called Biker Wars in Quebec. Before 9/11, Canadian officials co-operated with Americans in Washington State on border security issues in the form of an Integrated Border Enforcement Team (IBET) in British Columbia. The IBET model, too, was expanded across the country after 9/11. In the jurisdictions where they were established as a federal government "horizontal initiative" as part of new anti-terrorism funding (T. B. of C. Government of Canada 2014), the INSETs replaced the RCMP's National Security Investigations Sections. They were first mentioned in the media only a month after 9/11 (Steinbachs 2001), and formally launched in June of 2002 (Woods 2002). They were permanently funded in 2007. The INSETs have a mandate for collecting and sharing intelligence among partners, enforcing laws related to national security, and enhancing Canada's capacity to combat national security threats. Each INSET comprises representatives from the RCMP, CSIS, CBSA, and provincial and municipal police forces. An initial set of INSETs were created in Vancouver, Toronto, Ottawa, and Montreal, with a new one created in Edmonton 2012.

Beginning in 2004, the idea of integration began to permeate commentary in policing jour-

nals and professional associations. Municipal police, in particular, lamented their lack of involvement in national security (Canadian Association of Chiefs of Police 2004, 34). In these early documents, integration is presented as a necessary response to the links between local crime and global threats (Canadian Association of Chiefs of Police 2004, 34), but is also clearly about institutional competition for resources: the CAPB, in a submission from the Vancouver Police Board, laments at length the fact that Canada's national security strategy, *Securing an Open Society* (Canada Privy Council 2010), omitted the role of municipal police–and the need to fund them–from its consideration of counter-terrorism in Canada (Canadian Association of Police Boards 2004, Annex C). There was a strong sense that the drive to integration was not being matched with a governance structure to ensure the recognition of each others' roles and responsibilities (Canadian Association of Chiefs of Police 2004, 33). Eventually, in 2007, the Canadian Association of Chiefs of Police, together with CSIS, hosted a conference to come up with a set of principles for a "Common Framework for National Security" for Canadian law enforcement agencies, which stated that they would use "integration as the foundation of LE's [law enforcement's] strategy to investigate NS [national security] criminal activities" (Canadian Association of Chiefs of Police 2007, 6–12). By this time the idea of integration was well-entrenched, and the concept had a central role in Canada's counter-terrorism strategy released in 2011, *Building Resilience Against Terrorism* (Government of Canada 2013).

The most important facilitating condition for integration in Canada was the terrorist attacks of 9/11. A few days after the attacks, the RCMP initiated "Project Shock", a task force dedicated to tracking all the public's tips about terrorism in the immediate aftermath of 9/11. This was eventually expanded into Project A-O Canada (named for the RCMP divisions involved), the initiative that infamously shared information in unauthorized ways with American officials, ultimately resulting in the detention of Maher Arar. Falconer and Mathai (2006) argue that the mandate of prevention (of terrorist attacks) quickly came to overshadow the RCMP's traditional mandate of prosecution, and that the culture of national security within the RCMP shifted quickly to one in which the "rules that governed transmittal of information no longer applied" (Falconer and Mathai 2006, 57). This culture was entrenched, they argue, with the passage of Bill

C-36, the Anti-Terrorism Act, that granted the RCMP new powers of investigation and created specific terrorism offences in the criminal code (Falconer and Mathai 2006, 60). This prevention culture created the conditions of possibility that allowed the RCMP to investigate Maher Arar on the slimmest of suspicions. This distinction between a national security intelligence investigation and a national security criminal investigation became important in Justice O'Connor's report into the Arar investigations, and ultimately the basis for institutional changes in how the RCMP and CSIS work together (Falconer and Mathai 2006, 61).

There was a general consensus among the interviewees that Canada was not headed down the path of integrated policing units; that is, there would not have been INSETs had 9/11 not happened. Rather than being explicitly modeled on any of the previous integrated units, the inspiration for INSETs seems to have been community policing: the idea that terrorism was such a complicated phenomenon that, as in community policing, all stakeholders needed to be involved. INSETs and IBETs were created quickly.

The other major facilitating condition for the creation of INSETs was the inflow of extra money for security after 9/11. New money for national security totaled $8 billion in the first five years after 9/11, of which $1.6 billion was allocated to intelligence and policing (Secret Service, 435). According to an Audit of the Public Security and Anti-Terrorism Initiative in 2009, thirty-five departments received $12.9 billion in funding between 2001 and 2009 (Fitzpatrick 2013). Without this influx of funds, the number of individuals working on security within the RCMP is unlikely to have bloomed in the way that it did: immediately following the split between the RCMP and CSIS in 1985, approximately twelve individuals worked on national security criminal investigations in the RCMP headquarters (Anonymous interview, 2013); by the time of the Arar investigation in 2004, Toronto's INSET alone, for instance, comprised of fifty-three RCMP members, two RCMP civilian employees, and twenty-two seconded employees from other security agencies (Whitaker, Kealey, and Parnaby 2012, 441).

Two Commissions of Inquiry were also fundamentally important for the development of national security policing, the operation of the INSETs, and information sharing after 9/11: the

Major Commission on the Air India bombings, and the O'Connor Commission on the Maher Arar investigations. The O'Connor Commission reported first, making a number of recommendations to the RCMP and the Canadian government. Most importantly for the purposes of this paper, it mandated a clear delineation between the activities of the RCMP and CSIS. In response, the RCMP and CSIS signed a Memorandum of Understanding outlining their respective mandates and how they would co-operate in future–through a process of deconfliction at the highest levels (RCMP National Security Criminal Investigations 2009; Blaze Carlson, Hui, and Thanh Ha 2013). The process of integrating intelligence and policing became more formalized and more process driven (anonymous interview, 2013). While this trend to formalization might have resulted independently from the desire of municipalities for recognition, it is clear from the documents and from interviews that the O'Connor Commission is the direct precursor to the formalization of co-operation between the RCMP and CSIS.

The Major Commission into the Air India bombings and the subsequent investigation had related, but with somewhat different conclusions. The lesson of Air India seemed to be that the RCMP and CSIS co-operated poorly by failing to share information, by duplicating threat assessment structures in inefficient ways, and by failing to appreciate the differences between intelligence and evidence (Major 2010). The major challenge for the RCMP's national security operations, in light of these reports, was to figure out how to co-operate enough to avoid another Air India, but in ways that would prevent another Maher Arar.

Trends in National Security Policing

i. Formalization

Several trends are clear from the foregoing institutional history. The first is the trend to formalization. The creation of the INSETs after 9/11, and the restructuring of the relationship between CSIS and the RCMP after the Arar investigations, both have the intention of making sure that all stakeholders are part of decision-making, but that none oversteps its boundaries. Several interviewees noted that this trend to formalization meant that co-operation in national security policing in Canada has become more process driven. They highlighted the importance of formal-

ization in making sure that all laws, rules, and regulations are followed (anonymous interviews, 2013). However, what the trend to formalization means for informal co-operation remains uncertain. Research in other jurisdictions suggests that much policing co-operation happens at the informal, rather than the formal, level (Guille 2010; Yon 2010; see also Dunton and Kitchen 2014). Personal contacts play a pivotal role, and while formalization associated with centralization (such as the MOU between CSIS and the RCMP) may serve to limit informal contacts, formalization associated with integration (such as the INSETs) may, in fact, increase opportunities for trust building and informal information sharing. Sheptycki and Bowling (2012) call this the difference between "law in books" and "law in action" (42). Integration may create the conditions of possibility for informal co-operation.

ii. Co-ordination

A clear stated goal of the *Common Framework for National Security* is the co-ordination of media engagements, political briefings, and extra-territorial national security criminal investigations (Canadian Association of Chiefs of Police 2007, 11). One interviewee noted the importance of new skills in national security investigations that members of municipal police departments seconded to INSETs learn and then take back to their home law enforcement organizations (anonymous interview, 2013). Such skills building may be important to avoiding breaches of protocol and ethics; Falconer and Mathai (2006) directly connect the lack of trained national security investigators after 9/11 with the errors that led to Maher Arar's rendition.

However, the goal of speaking with one voice may have its dangers as well. The Major Commission notes that Government representatives spoke with one voice before the Commission, meaning that even when there were known differences of opinion, the Commission could not always get a handle on what they were (Major 2010, 6). Given that the Chiefs of Police also mandated to speak with one voice, productive disagreement may disappear in the face of institutional protection. This is dangerous not merely because it hides disagreements. A group that seeks to find a single message is also in danger of coming to think the same way. Security professionals are already prone to seeing the world through a single lens; applying a national security frame is

not always appropriate. As security officials are trained in similar ways to create common rules and procedures, and become subject to groupthink, they are likely to begin analyzing problems in similar ways and proposing particular kinds of (national security) solutions (Bigo 1996; see also Kitchen forthcoming). It does not benefit Canada at large when everyone thinks the same way. An example of this kind of danger emerged during the G20 in Toronto, when intelligence and training documents blurred the distinctions between protesters, anarchists, and terrorists; an after-action review argued that one of the reasons the G20 protest turned violent was that police officers were primed to expect it (Kitchen and Rygiel n.d.).

iii. Information gathering and sharing

A third clear trend, and a by-design outcome of the push to the creation of integrated institutions, is the gathering of more and more information about Canadian citizens and foreigners. While information gathering by CSEC has been particularly controversial lately (Freeze 2013), there are more general risks to the accumulation of data. One interviewee, when asked to comment on the diagnoses of the problem of terrorism as one of "connecting the dots", noted that it was instead more like identifying a single grain of sand in a windstorm (anonymous interview, 2013). Having more data does not necessarily make information easier to find. In fact, it may make it harder. More data shared more widely means that errors may be magnified before they can be corrected (Citron and Pasquale 2011). There is a risk to citizens, then, of gathering too much data. There is some evidence that the RCMP's national security program faces these problems associated with data gathering. A report from the Privacy Commissioner in 2008 found that RCMP databanks of files exempt from public access were not being reviewed on a regular basis as required by law, and that fifty percent of the files in the audit sample that classified as exempt for reasons of national security ought not to have remained in the databank (Office of the Privacy Commissioner of Canada 2008).

Relatedly, the integration of data and of institutions has not been widely matched by an integrated review and complaints mechanism. The O'Connor Commission report recommended the creation of a new, integrated review mechanism be created, allowing citizens a one-stop shop

for complaints, and a mechanism that could review integrated operations (O'Connor n.d., 22). This was re-iterated in a Special Report to Parliament from the Privacy Commissioner's Office in January 2014, which re-iterated the importance of implementing the findings of the Major and O'Connor Commissions, and also of matching co-operation among intelligence agencies with co-operation among review boards (Office of the Privacy Commissioner of Canada 2014). This is a clear gap in government accountability mechanisms, which makes it harder for citizens to complain about their government, and harder to achieve necessary democratic oversight.

Conclusion

The overwhelming take-away point from this research is that the evaluation of counter-terrorism from a critical perspective must be more tentative and less definitive than the evaluation of counter-terrorism from a rationalist perspective. It is very difficult to evaluate a counter-terrorist policy on the basis of whether or not it reduces terrorism or terrorist activity. The failure of rational calculus, the securitizing discourses that surround most counter-terrorism policy, and the fact that counter-terrorism policy can have unintended outcomes all mean that such perspectives are rendered meaningless from a critical perspective. The logic of security and the politics of security research, together with the inherent biases of the researcher, will all influence outcomes. No two attempts at evaluating effectiveness will be exactly the same, because the researcher and the objects and subjects of research will face different circumstances. Critical effectiveness research may not be replicable, but it can be systematic and transparent.

A critical perspective makes it clear that understanding the technical or managerial aspects of effectiveness is insufficient without understanding societal effects. If, as much of the literature has hypothesized, the war on terrorism is a generational struggle, then we must take into account both short and long-term effects of policies and institutional arrangements. In Canada, we are only just beginning to understand the implications of all the institutional changes we enacted after 9/11. There is much we do not know, and much we may never know. Initial research suggests that while we may have successfully corrected some of the excesses of the immediate post-9/11 period, and some of the errors of the Arar investigations, more subtle and insidious effects related to formalization, co-ordination, and information gathering may yet exist.

References

Aradau, Claudia, and Rens Van Munster. 2007. Governing terrorism through risk: Taking precautions, (un)knowing the future. *European Journal of International Relations* 13 (1): 89–115. doi:10.1177/1354066107074290.

Beck, Ulrich. 2006. Living in the world risk society. *Economy and Society* 35 (3): 329–45.

Bell, Colleen. 2011. *Freedom of security, the: Governing Canada in the age of counter-terrorism*. Vancouver, B.C.: UBC Press.

Bigo, Didier. 1996. *Polices En Réseaux : L'expérience Européenne*. Paris: Presses de Sciences Po.

Blaze Carlson, Kathleen, Anna Hui, and Tu Thanh Ha. 2013. How three London teens ended up dead or jailed, accused of terrorism. *The Globe and Mail*, April 6. http://www.theglobeandmail.com/news/national/how-three-london-teens-ended-up-dead-or-jailed-accused-of-terrorism/article10825822/?page=all.

Boutilier, Alex. 2014. Ottawa has slapped a life-long gag order on bureaucrats and lawyers working in a number of government agencies dealing with sensitive national security information. *The Toronto Star*, March 13. http://www.thestar.com/news/canada/2014/03/13/ottawa_imposes_linelong_gag_order_on_bureaucrats_lawyers.html.

Bowling, Ben, and James Sheptycki. 2012. *Global policing*. Thousand Oaks, CA: SAGE Publications.

Buzan, Barry, Ole Waever, and Jaap De Wilde. 1997. *Security: A new framework for analysis*. Boulder, C.O.: Lynne Rienner Pub.

Canada Privy Council. 2010. *Securing an Open Society: Canada's National Security Policy*. Ottawa: Government of Canada. Privy Council Office. http://books.scholarsportal.info.proxy.lib.uwaterloo.ca/viewdoc.html?id=22642.

Canadian Association of Chiefs of Police. 2004. *Resolutions Adopted at the 99th Annual Conference*. Vancouver, BC: Canadian Association of Chiefs of Police. http://www.cacp.ca/media/resolutions/efiles/38/Resolution2004Eng.pdf.

———. 2007. *Resolutions Adopted at the 102nd Annual Conference*. Calgary, AB: Canadian Association of Chiefs of Police. http://www.cacp.ca/media/resolution

s/efiles/38/EnglishResolutions_Package_2007.pdf.

Canadian Association of Police Boards. 2004. *Resolutions Approved at the Canadian Association of Police Boards Annual Meeting*. http://capg.ca/wp-content/uploads/2013/05/2004_CAPB_Resolutions.pdf.

Citron, Danielle Keats, and Frank Pasquale. 2011. Network accountability for the domestic intelligence apparatus. *Hastings Law Journal* 62 (March). http://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=1990&context=fac_pubs.

Crenshaw, Martha. 2010. *The consequences of counterterrorism*. New York: Russell Sage Foundation.

Department of Homeland Security. 2010. *2010 Baseline Capabilities Assessment of Fusion Centers and Critical Operational Capabilities Gap Mitigation Strategy*. Department of Homeland Security. https://www.dhs.gov/2010-baseline-capabilities-assessment-fusion-centers-and-critical-operational-capabilities-gap.

———. 2012. National network of fusion centers fact sheet. *Homeland Security*. Accessed March 27, 2014. http://www.dhs.gov/files/programs/gc_1296484657738.shtm.

Dunton, Caroline, and Veronica Kitchen. 2014. Paradiplomatic policing and relocating Canadian foreign policy. *International Journal: Canada's Journal of Global Policy Analysis* March: 0020702014525903. doi:10.1177/0020702014525903.

Falconer, Julian N., and Sunil S. Mathai. 2006. The anti-terrorism act and the Arar findings: Democracy protected or democracy eroded? *National Journal of Constitutional Law* 21: 49–58.

Fitzpatrick, Meagan. 2013. Canada can't account for $3.1B in anti-terror funding, AG finds. *CBC News*, April 30, online edition. http://www.cbc.ca/1.1303999.

Freeze, Colin. 2013. How CSEC became an electronic spying giant. *The Globe and Mail*, November 30. http://www.theglobeandmail.com/news/politics/how-csec-became-an-electronic-spying-giant/article15699694/.

Gerspacher, Nadia, and Benoit Dupont. 2007. The nodal structure of international police cooperation: An exploration of transnational security networks. *Global Governance: A Review of Multilateralism and International Organizations* 13 (3): 347–64.

Gill, Peter. 2009. The intelligence and security committee and the challenge of security networks. *Review of International Studies* 35 (4): 929–41. doi:10.1017/S0260210509990362.

Government of Canada. 2013. *Building Resilience Against Terrorism*. Department of Public Safety, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-gnst-trrrsm/rslnc-gnst-trrrsm-eng.pdf.

Government of Canada, Public Works and Government Services Canada (P. W. and G. S. C.). 2014. *Order Amending the Schedule to the Security of Information Act*. *Canada Gazette*. Accessed March 12, 2014. http://www.gazette.gc.ca/rp-pr/p2/2014/2014-03-12/html/sor-dors35-eng.php.

Government of Canada, Treasury Board of Canada (T. B. of C.). 2014. *Horizontal Initiative: Integrated National Security Enforcement Teams (INSET)*. Accessed April 5, 2014. http://www.tbs-sct.gc.ca/hidb-bdih/initiative-eng.aspx?Hi=76.

Guille, Laure. 2010. Police and judicial cooperation in Europe: Bilateral versus multilateral cooperation. In *International Police Cooperation: Emerging Issues, Theory and Practice*, edited by Frédéric Lemieux, 25–41. Portland, OR: Willan Publishing.

Huysmans, Jef. 2006. *The politics of insecurity: Fear, migration and asylum in the EU*. New York: Routledge.

Institute of Race Relations. 2010. Evidence to the UK parliamentary select committee inquiry on preventing violent extremism. *Race & Class* 51 (3): 73–80. doi: 10.1177/0306396809361272.

Jiao, Allan Y., and Harry M. Rhea. 2007. Integration of police in the United States: Changes and development after 9/11. *Policing & Society* 17 (4): 388–408.

Kitchen, Veronica. forthcoming. The ethics of mega-event security: When the world comes to visit. In *Ethics and Security in Canadian Foreign Policy*, edited by Rosalind Warner. Vancouver, B.C.: UBC Press.

Kitchen, Veronica, and Adam Molnar. n.d. The promise and perils of integrated models of public safety in Canada (unpublished paper under review, publication forthcoming, June 9, 2014). In *Researching Terror Networks: From Radicalization to Counter-Terrorism Policies*, edited by Martin Bouchard.

Kitchen, Veronica, and Kim Rygiel. n.d. Integrated security networks: Less not more accountability (unpublished paper, forthcoming, June 9, 2014). In *The State on Trial: Policing Protest at the G20 and Beyond*, edited by Margaret Beare. Vancouver, B.C.: UBC Press.

Lindekilde, Lasse. 2012. Introduction: Assessing the effectiveness of counter-radicalisation policies in northwestern Europe. *Critical Studies on Terrorism* 5 (3): 335–44. doi:10.1080/17539153.2012.723522.

Lum, Cynthia, Leslie W. Kennedy, and Alison Sherley. 2006. Are counter-terrorism strategies effective? The results of the Campbell Systematic Review on counter-terrorism evaluation Research. *Journal of Experimental Criminology* 2: 489–516.

Major, John C. 2010. Final report | Commission of Inquiry into the investigation of the bombing of Air India Flight 182. *Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182*. Accessed June 17, 2014. http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/air_india/2010-07-23/www.majorcomm.ca/en/reports/finalreport/default.htm.

McCulloch, Jude, and Sharon Pickering. 2009. Pre-crime and counter-terrorism: Imagining future crime in the "War on Terror." *British Journal of Criminology* 49: 626–45. doi:10.1093/bjc/azp023.

Minsky, Amy. 2013. RCMP stops responding to people using access to information laws: Information commissioner. *Global News*, August 16. http://globalnews.ca/news/785556/rcmp-stopped-responding-to-information-requests-information-commissioner/.

Monaghan, Jeffrey, and Kevin Walby. 2012. Making up "terror identities": Security, intelligence, Canada's integrated threat assessment centre and social movement suppression. *Policing and Society: An International Journal of Research and Policy* 22 (2): 133–51.

Mueller, John, and Mark G. Stewart. 2011. *Terror, security, and money: Balancing the risks, benefits, and costs of homeland security*. Oxford, UK: Oxford University Press.

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

O'Connor, Dennis. *A New Review Mechanism for the RCMP's National Security Activities*. Ottawa: Commission of Inquiry into the actions of Canadian officials in relation to Maher Arar. Library & Archives Canada, Online. http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.ararcommission.ca/eng/EnglishReportDec122006.pdf.

Office of the Privacy Commissioner of Canada. 2008. *Backgrounder: Audit Report of the Privacy Commissioner of Canada - Examination of RCMP Exempt Data Banks (February 13, 2008)*. http://www.priv.gc.ca/media/nr-c/2008/nr-c_b-di_080213_e.asp.

———. 2014. *Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance - Special Report to Parliament - January 28, 2014.* Ottawa: Office of the Privacy Commissioner of Canada. http://www.priv.gc.ca/information/sr-rs/201314/sr_cic_e.asp#toc.

Pantucci, Raffaello. 2010. A contest to democracy? How the UK has responded to the current terrorist threat. *Democratization* 17 (2): 251–71.

Perl, Raphael. 2007. *Combating Terrorism: The Challenge of Measuring Effectiveness.* CRS Report for Congress. Washington, DC: Congressional Research Service - Library of Congress.

RCMP National Security Criminal Investigations. 2009. *RCMP Actions in Response to Recommendations Stemming from the Report of the Events Relating to Maher Arar (O'Connor Inquiry)*. Ottawa: Royal Canadian Mounted Police. http://www.rcmp-grc.gc.ca/nsci-ecsn/oconnor-eng.pdf.

Schneider, Stephen, and Christine Hurst. 2008. Obstacles to an integrated, joint forces approach to organized crime enforcement: A Canadian case study. *Policing: An International Journal of Police Strategies & Management* 31 (3): 359–79. doi:10.1108/13639510810895759.

Steinbachs, John. 2001. Police forces team up. *The Ottawa Sun*, October 31, Final Edition edition, sec. News.

Van Dongen, T.W. 2011. Break it down: An alternative approach to measuring effectiveness in counterterrorism. *Journal of Applied Security Research* 6: 357–71.

Van Um, Eric, and Daniela Pisoiu. 2011. *Effective Counter-Terrorism: What Have We Learned So Far?* (Economics of Security Working Paper 55). Berlin: Economics of Security. http://www.diw.de/documents/publikationen/73/diw_01.c.386651.de/diw_econsec0055.pdf.

Whitaker, Reginald, Gregory S Kealey, and Parnaby. 2012. *Secret service: Political policing in Canada : From the Fenians to fortress America*. Toronto: University of Toronto Press.

Woods, Allan. 2002. Four anti-terror squads launched. *The Globe and Mail*, June 18, sec. C.

Yon, Hasan. 2010. Police liaisons as builders of transnational security co-operation. In *Emerging Transnational (In)security Governance: A Statist-Transnationalist Approach*, edited by Ersel Aydinli, 1st ed. 124–42. New York: Routledge.