SCHOOL OF LAW
CASE WESTERN RESERVE UNIVERSITY

Canada-United States Law Journal

Volume 37 | Issue 2 Article 12

January 2012

Beyond the Border Action Plan: A Tool for Enhanced Canada-U.S. Cooperation on Critical Infrastructure and Cyber Security - Or More Window Dressing, The

William de Laat

THE BEYOND THE BORDER ACTION PLAN: A TOOL FOR ENHANCED CANADA-U.S. COOPERATION ON CRITICAL INFRASTRUCTURE AND CYBER SECURITY – OR MORE WINDOW DRESSING?

*By William de Laat**

While there is ample recognition in both countries of the deep integration of the Canadian and American economies, our mutual reliance on an intricate web of interconnected physical and cyber infrastructure is often overlooked. With few exceptions, governments and the private sector have a limited understanding of the complex interdependencies between these shared systems and networks, and the enormous economic fallout that can result from major infrastructure failures.

Canada and the United States have made only modest progress to date in addressing issues related to their shared critical infrastructures and cyber systems. Neither country has devoted sufficient resources nor shown a sustained commitment to making shared infrastructures more resilient and less vulnerable to failure or attack.

Both governments have been slow to put in place effective policies and procedures to anticipate, manage, and recover from major cross-border infrastructure disruptions. Joint initiatives in the *Beyond the Border* Action Plan ("BTBAP")[1] and the *Canada-United States Action Plan for Critical Infrastructure* ("CUSCI"),[2] have not been given priority by senior officials in either country and have failed to set out a coherent set of deliverables, deadlines, and accountabilities. This, in turn, has left private sector stakeholders to fend largely for themselves, with little direction from government.

---

* William de Laat is currently an International Security and Government Relations Consultant at De Laat Global Strategic Consulting. Prior to this, he served as Counsellor in the Public Safety and Border Security division at the Canadian Embassy in Washington, D.C.

1. BEYOND THE BORDER: A SHARED VISION FOR PERIMETER SECURITY AND ECONOMIC COMPETITIVENESS (2011), *available at* http://www.whitehouse.gov/sites/default/files/us-canada_btb_action_plan3.pdf [hereinafter BTB].

2. CANADA-UNITED STATES ACTION PLAN FOR CRITICAL INFRASTRUCTURE (2010), *available at* http://www.publicsafety.gc.ca/prg/ns/ci/fl/cnus-ct-pln-eng.pdf [hereinafter CUSCI].

Canada and the United States should address these issues as a top priority immediately after the 2012 United States presidential elections. By moving aggressively to identify gaps and vulnerabilities, and to agree on remedial measures to protect their joint systems and networks, they will not only be protecting their respective economic and security interests, but they could also become important models for international cooperation in this area. In the global rush to determine cyber security standards, Canada, in particular, should ramp up its game, or it might well face the bleak prospect of being left out in the cold while the United States and other global players move ahead without them.[3]

CONTEXT

At the outset, I wish to stress that the views and opinions expressed here are strictly my own. I recognize that a short article like this can provide only a quick and incomplete picture of Canada-United States relations in critical infrastructure protection and cyber security. My purpose in writing this article is to suggest where there might be opportunities for making more rapid progress and to identify some possible gaps and weaknesses in our current approach.

CRITICAL INFRASTRUCTURE AND CYBER SECURITY AS PRIORITY ISSUES FOR PUBLIC POLICY

Sometimes the terms critical infrastructure and cyber security are confused and misunderstood even by the public policy makers responsible for them. It is a truism to point out that networks, systems, and information flows have become the lifeblood of the global economy. But few seem to be aware that *almost all* business, economic, and even personal information now exists in digital form. The implications of this fact are staggering.

And so, the links between infrastructure protection, cyber security, and trade are unmistakable. As President Obama recently stated, "America's economic prosperity in the 21st century will depend on cyber security."[4] Another expert report put it this way:

3. *See generally, e.g.*, *Ottawa Needs to Improve Cyber Security: Auditor General*, GLOBE & MAIL (Oct. 23, 2012, 7:30 PM), http://www.theglobeandmail.com/commentary/editorials/ottawa-needs-to-improve-cyber-security-auditor-general/article4632711/ (discussing Canada's need to improve its cyber security standards and to place a higher profile on efforts to do so).

4. Press Release, Off. of the Press Sec'y, The White House, Remarks by the President on Securing Our Nation's Cyber Infrastructure (May 29, 2009)(on file with author), *available at* http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

The U.S. has developed more than most other nations as a modern society heavily dependent on electronics, telecommunications, energy, information networks, and a rich set of financial and transportation systems that leverage modern technology. This asymmetry is a source of substantial economic, industrial, and societal advantages, but it creates vulnerabilities and critical interdependencies that are potentially disastrous to the United States.[5]

Stand-alone critical infrastructure, unconnected to the Internet or other large computer networks, is almost non-existent today.

In a Canada-United States context, these networks and systems—be they computer networks, electric power grids, pipelines, transportation and logistics networks, or supply chains—together form the essential underpinnings of an immense and highly prosperous North American economy. Andrew Graham, a Canadian policy commentator, underlines this convergence of cyber systems and critical infrastructure: "the interdependence of critical CI systems is developing an overlay of what might be called the meta-CI system, cybernetics and computer control systems that control . . . systems such as energy, transportation, finance, and others."[6]

It seems that not a day goes by without increasingly alarming reports of intrusions and disruptions of banking systems or government networks. This is remarkable, given that back issues of the *Canada-United States Law Journal, for example,* reveal almost no references to critical infrastructure or cyber security until a couple of years ago.[7] Major disruptions or failures of critical infrastructure have never really loomed large in the public psyche, and as a result, these issues were never at the forefront of public policy. Today, however, growing public and business concern about the potential economic

5. JOHN S. FOSTER, JR. ET AL., REPORT OF THE COMMISSION TO ASSESS THE THREAT TO THE UNITED STATES FROM ELECTROMAGNETIC PULSE (EMP) ATTACK 2 (2004), *available at* http://www.empcommission.org/docs/empc_exec_rpt.pdf.

6. ANDREW GRAHAM, MACDONALD-LAURIER INST., CANADA'S CRITICAL INFRASTRUCTURE: WHEN IS SAFE ENOUGH SAFE ENOUGH? 2 (2011), *available at* http://www.macdonaldlaurier.ca/files/pdf/Canadas-Critical-Infrastructure-When-is-safe-enough-safe-enough-December-2011.pdf.

7. See Carmine Marcello, *Keynote Luncheon Address II: Keynote Address*, 36 CAN.-U.S. L.J. 114 (2012); see also Stephen E. Flynn, *The New Reality in Canada/U.S. Relations: Reconciling Security and Economic Interests and the Smart Border Declaration*, 29 CAN.-U.S. L.J. 9 (2003); see also Theodore C. Theofrastous, *Security and the Economy: The North American Computer and Communication Infrastructure*, 29 CAN.-U.S. L.J. 225 (2003).

impacts of infrastructure disruptions is becoming a compelling driver for speeding up joint work between our two countries in this area.[8]

Another indication of growing policy interest in cyber security is found in a survey of a large cross-section of global public policy leaders conducted by the Security and Defence Agenda of Brussels, Belgium.[9] Here are some of the survey's key findings:

- Forty-five percent of respondents said cyber security is now as important as border security.[10]
- Forty-three percent of respondents identified damage or disruption to critical infrastructure and its potential economic impact as the greatest single threat posed by cyber attacks.[11]
- Fifty-seven percent of respondents believed an arms race is taking place in cyberspace.[12]
- Thirty-six percent of respondents said cyber security is more important than missile defence.[13]
- The cyber-readiness of the United States, Canada, Australia, United Kingdom, China, and Germany, all lagged behind smaller nations like Israel, Sweden, and Finland, among the twenty-three countries rated by report.[14]

As a result, critical infrastructure protection, and to an even greater extent, cyber security, have become increasingly important public policy priorities.[15] This not only creates enormous opportunities

8. *See, e.g.*, AUD. GEN. OF CAN., CHAPTER 3: PROTECTING CANADIAN CRITICAL INFRASTRUCTURE AGAINST CYBER THREATS, FALL REPORT OF THE AUDITOR GENERAL OF CANADA (2012), *available at* http://www.oag-bvg.gc.ca/internet/docs/parl_oag_201210_03_e.pdf.

9. *See* BRIGID GRAUMAN, SEC. & DEF. AGENDA, CYBER SECURITY: THE VEXED QUESTION OF GLOBAL RULES (2012), *available at* http://www.mcafee.com/us/resources/reports/rp-sda-cyber-security.pdf.

10. *Id.* at 47.

11. *Id.*

12. *Id.*

13. *Id.*

14. *See generally id.* at 51-85.

15. *See, e.g.*, CONF. BD., PROTECTING CRITICAL INFRASTRUCTURE: A CROSS-BORDER ACTION PLAN (2009), *available at* http://issuu.com/emergency-solutionsintl/docs/cross#download; *see also, e.g.*, PUB. POL'Y FORUM, CYBER-SECURITY: DEVELOPING A CANADIAN STRATEGY (2008), *available at* http://old.ppforum.ca/common/assets/publications/fr/20085161235 12.pdf.

for ramping up our work on these issues, but it also poses major challenges and raises expectations of those responsible for managing them.

If these were easy issues, they would have been solved a decade ago. But there really are no easy solutions or "low-hanging fruit" here. Critical infrastructure and cyber security issues are difficult to grapple with. They are complex and constantly changing. Added to this complexity is the fact that none of these networks or infrastructures falls exclusively within the public safety, law enforcement, intelligence, or trade domains. This lack of clear accountabilities and a poor understanding by many policy makers of the complex issues at play have made policy development slow and cumbersome. To make things even messier, these infrastructure set are more often controlled by the private sector or provincial and state players than by federal government so.

A BRIEF REVIEW OF CANADA-UNITED STATES COLLABORATION ON CYBER SECURITY AND CRITICAL INFRASTRUCTURE

The United States and Canada have had a long history of collaboration on critical infrastructure, emergency management, and defence issues.[16] It is instructive to reflect on how our joint work on critical infrastructure and cyber security has evolved, particularly since September 11, 2001. Before the 1990s, the term *infrastructure* was usually synonymous with public works (bridges, canals, etc.) or information systems. After September 11, however, the policy debate shifted from infrastructure *adequacy* to physical and cyber infrastructure *protection*, and then more recently, to infrastructure *resilience*.

For all its hoopla, and, as many have said, waste of time and energy, Y2K was an important first step by Canada and the United States in working together to secure vital computer and telecommunications networks. That work brought about close collaboration across all sectors of the economy, innovative new forms of public-private sector cooperation, and for the first time in a cross-border setting, a serious assessment of the potential interdependencies and cascading effects that failures in one sector could have on others. The work plans associated with Y2K were rigorous, with contingency plans developed for almost everything that might go wrong.[17] The

16. *See, e.g.*, U.S. DEP'T OF HOMELAND SEC. & PUB. SAFETY CAN., COMPENDIUM OF U.S.-CANADA EMERGENCY MANAGEMENT ASSISTANCE MECHANISMS (2012), *available at* http://www.publicsafety.gc.ca/prg/ns/ci/_fl/cuc-emam-eng.pdf.

17. *See, e.g.*, Lance B. Eliot, *Y2K Late-Date Solution: Business Contingency Planning*, 30 DEC. LINE 13, 13-14 (2009), *available at*

entire effort had a strong economic focus and enjoyed sustained high-level political support.[18]

It also marked the tentative beginning of a new global awareness of these issues. An International Y2K Cooperation Centre[18] was established at the behest of national Y2K coordinators from over 120 countries when they met at the First Global Meeting of National Y2K Coordinators at the United Nations in December 1988.[19] The World Bank provided funding.[20] The Centre's mission was to "promote increased strategic cooperation and action among governments, peoples, and the private sector to minimize adverse Y2K effects on the global society and economy."[21]

Though the problem at hand at that time was more static and less complex than the ones we face in dealing with critical infrastructure and cyber security today, Y2K did drive our two countries to establish joint steering committees and several private-public sector working groups to address a similar, common threat.[22] Whether the investment of money and energy was ultimately warranted may never be known, but it did lay the groundwork for future cooperation.

Issues related to critical infrastructure protection took on added urgency after the September 11 attacks, though differences between Canada and the United States over the justification for invading Iraq and Canada's refusal to join the "coalition of the willing" put a significant damper on Canada-United States security relations.[23] The

---

http://www.decisionsciences.org/DecisionLine/Vol30/30_1/info30_1.pdf (discussing methods for drafting contingency plans for different potential scenarios as a result of Y2K).

18. *See, e.g.*, U.S. GEN. ACCT. OFF., YEAR 2000 COMPUTING CRISIS: BUSINESS CONTINUITY AND CONTINGENCY PLANNING (1998), *available at* http://www.gao.gov/special.pubs/bcpguide.pdf.

18 INT'L Y2K COOPERATION CTR., http://www.iy2kcc.org/ (last visited Dec. 16, 2012).

19. *See* Elisabeth Kaplan et al., *Historical Note, International Y2K Cooperation Center Records 1998-2000*, UNIV. OF MINN., http://special.lib.umn.edu/findaid/xml/cbi00153.xml (last visited Dec. 16, 2012).

20. *See id.*

21. *Id.*

22. *See generally* U.S. DEP'T OF COMM., THE ECONOMICS OF Y2K AND THE IMPACT ON THE UNITED STATES (1999), *available at* http://www.esa.doc.gov/sites/default/files/reports/documents/y2k_1.pdf (discussing various joint-initiatives the United States had with Canada to minimize the adverse effects and costs of Y2K).

23. *See generally* THOMAS S. AXWORTHY, CAN. DEF. & FOREIGN AFF. INST., UNWILLING TO BE WILLING: THE PRIMACY AND CAPABILITY PRINCIPLES IN

"Patriot Act"[24] and the unhelpful "good versus evil" and "you're either with us or against us" positioning of the Bush Administration caused concerns among many Canadians about the potential impact that new United States security arrangements would have on Canadian sovereignty and values, especially personal privacy.[25]

At the time I took up my position as Counsellor for Public Safety and Border Security at the Canadian Embassy in Washington, D.C. in 2003, relations between the two countries were markedly cool. However, due to the personal energy and drive of Homeland Security Secretary Tom Ridge and Deputy Prime Minister John Manley, joint work between the two countries moved forward under the Smart Border Accord.[26] This served to underscore the important role that personal relationships and direct involvement of senior leaders can have in addressing joint security and economic issues, even in the face of prickly bilateral relations.

Action Item 21 of the Smart Border Accord required the American and Canadian Governments to "[c]onduct binational threat assessments on trans-border infrastructure and identify necessary additional protection measures, and initiate assessments for transportation networks and other critical infrastructure."[27] Joint assessments were carried out in several sectors, including pipelines, electricity and transportation.[28]

In 2001, the two governments agreed on a *Joint Framework for Canada-United States Cooperation on Critical Infrastructure Protection* with a bi-national Steering Committee, to assess threats to "shared critical infrastructure and ensure an ongoing, high-level focus on the issue by both governments." The Steering Committee created

---

CANADIAN-AMERICAN RELATIONS (2003), *available at* http://www.cdfai.org/PDF/Unwilling%20To%20Be%20Willing.pdf (discussing the effect that Canada's refusal to join the "coalition of the willing" had on Canada-United States relations).

24. USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

25. *See, e.g.*, TREAS. BD. OF CAN. SEC., PRIVACY MATTERS: THE FEDERAL STRATEGY TO ADDRESS CONCERNS ABOUT THE USA PATRIOT ACT AND TRANSBORDER DATA FLOWS (2006), *available at* http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/pm-prp/pm-prp-eng.asp.

26. THE CANADA-U.S. SMART BORDER DECLARATION: ACTION PLAN FOR CREATING A SECURE AND SMART BORDER (2001), *available at* http://www.collectionscanada.gc.ca/webarchives/20071213014139/http://www.dfait-maeci.gc.ca/anti-terrorism/actionplan-en.asp.

27. *Id.* at Item 21.

28. *See, e.g.*, FOREIGN AFF. & INT'L TRADE CAN., SMART BORDER ACTION PLAN STATUS REPORT (2004), *available at* http://www.collections-canada.gc.ca/webarchives/20051229033040/http://www.dfait.gc.ca/can-am/main/border/status-en.asp [hereinafter STATUS REPORT].

working groups to draw up detailed work plans for collaboration in the areas of energy, telecommunications and transportation. A committee on cyber security was added later. The Steering Committee also established working groups "to address horizontal issues such as research and development, interdependencies, mapping and threat information sharing."[29]

This joint work on critical infrastructure was aided by the creation in Canada of the Office of Critical Infrastructure Protection and Emergency Management,[30] and in the United States, of the Office of Homeland Security in the White House.[31] Both were well placed strategically to ensure that there would be a high-level focus on critical infrastructure, including cyber security issues.

Another important milestone was the signing in 2004 of an Agreement Between the Government of the United States of America and the Government of Canada for Cooperation in Science and Technology for Critical Infrastructure Protection and Border Security.[32] But despite the momentum created by September 11, these efforts eventually faltered, due mainly to a series of reorganizations involving senior staff changes in both countries and a renewed focus by both governments on domestic infrastructure priorities.

The 2005 *Security and Prosperity Partnership of North America*[33] initiative made renewed attempts to address these issues and some limited progress was made, including the exchange of best practices, participation in joint exercises, and establishing mechanisms for coordinating emergency response and mutual assistance; yet, these

29. *See Policy Framework*, GOV'T OF CAN., http://www.nrcan.gc.ca/energy/sources/infrastructure/1563 (last visited Dec. 14, 2012).

30. *See, e.g.*, MICHEL ROSSIGNOL, PUB. SAFETY CAN., CRITICAL INFRASTRUCTURE PROTECTION AND EMERGENCY PREPAREDNESS (2001), *available at* http://publications.gc.ca/collections/Collection-R/LoPBdP/BP/prb017-e.htm (discussing the creation of the Office of Critical Infrastructure and Emergency Preparedness (OCIPEP) in February 2001).

31. *See, e.g.*, OFF. OF HOMELAND SEC., THE WHITE HOUSE, NATIONAL STRATEGY FOR HOMELAND SECURITY iv, 13, 47 (2002), *available at* http://www.ncs.gov/library/policy_docs/nat_strat_hls.pdf (discussing the creation of the White House Office of Homeland Security on October 8, 2001 and its purported mandate).

32. Agreement for Cooperation in Science and Technology for Critical Infrastructure Protection and Border Security, U.S.-Can., June 1, 2004, T.I.A.S. No. 04-601[hereinafter Science and Technology Agreement].

33. SECURITY AND PROSPERITY PARTNERSHIP OF NORTH AMERICA (2005), *available at* http://www.spp-psp.gc.ca/eic/site/spp-psp.nsf/eng/00057.html (a non-binding, information sharing initiative between the United States, Canada and Mexico, with a goal to increase both security and prosperity among the three nations).

were largely ad hoc activities, and not part of any comprehensive strategy.

However, cross-border work did continue in a few key sectors and geographic regions. The electricity sector, primarily as a result of fallout from the massive 2003 Northeast Blackout,[34] carried out joint work in identifying, assessing, and remediating vulnerabilities affecting the electrical grid, developed common reliability standards, and began work on cyber security standards.[35] Significant progress was also made in the transportation and broader energy sectors (oil and gas),[36] as well as at the regional level through organizations like the Pacific Northwest Economic Region.[37] In addition, several province-state partnerships were launched, including one involving Ontario and Michigan,[38] which have conducted joint exercises related to critical infrastructure in border areas.

During this period, both countries also continued to work together multilaterally in organizations like the North Atlantic Treaty Organization ("NATO"),[39] the G8,[40] the Asia-Pacific Economic Cooperation ("APEC"),[41] and the Organization of American States

34. *See, e.g.*, J. R. Minkel, *The 2003 Northeast Blackout–Five Years Later*, SCI. AM. (Aug. 13, 2008), http://www.scientificamerican.com/article.cfm?id=2003-blackout-five-years-later.

35. *See* STATUS REPORT, *supra* note 28; *see also* U.S. DEP'T OF ENERGY, U.S.-CAN. POWER SYS. OUTAGE TASK FORCE, FINAL REPORT ON THE AUGUST 14, 2003 BLACKOUT IN THE UNITED STATES AND CANADA: CAUSES AND RECOMMENDATIONS (2004), *available at* https://reports.energy.gov/BlackoutFinal-Web.pdf.

36. *See* STATUS REPORT, *supra* note 28.

37. PAC. NW. ECON. REG., http://www.pnwer.org/ (last visited Dec. 16, 2012).

38. *See, e.g.*, CAN.-U.S.-ONT.-MICH. BORDER TRANSP. P'SHIP, DETROIT RIVER INTERNATIONAL CROSSING STUDY (2008), *available at* http://www.partnershipborderstudy.com/pdf/EA-Report/EA_Chapter1.pdf (discussing the work of the Canada-U.S.-Ontario-Michigan Border Transportation Partnership, which consists of the United States Federal Highway Administration, Transport Canada, the Ontario Ministry of Transportation, and the Michigan Department of Transportation).

39. N. ATLANTIC TREATY ORG., http://www.nato.int/cps/en/natolive/index.htm (last visited Dec. 16, 2012).

40. *See, e.g.*, *Canada's G8 Website*, GOV'T OF CAN., http://www.canada-international.gc.ca/g8/index.aspx?view=d (last visited Dec. 16, 2012).

41. ASIA-PAC. ECON. COOPERATION, http://www.apec.org/ (last visited Dec. 16, 2012).

("OAS"),[42] to raise awareness and encourage national governments to step up their work in these areas.

Again, though some progress was made, it was difficult to sustain. Neither Canada nor the United States appeared willing to invest the time, energy, or resources needed to keep the momentum going, and neither side had effective champions to take ownership of these issues. One public commentator summed up the Canadian situation as follows:

> In the heady days after the 2001 tragedies, the federal government asserted a leadership role in protecting CI in Canada. What has emerged over the past 10 years, however, would appear to be little real progress . . . Seen from the outside, the efforts over that period had a stop-start quality, with more plans to plan than actual changes or results.[43]

Regarding joint Canada-United States activity during this period, the same commentator asked:

> [D]oes all of this activity with its array of committees, communications, and sharing of information actually constitute action? . . . While these efforts to build stronger ties are commendable and probably absolutely necessary, they are hardly the desired end state. What that state might look like remains unarticulated.[44]

WHAT EXACTLY DOES THE *BEYOND THE BORDER* ACTION PLAN COMMIT GOVERNMENTS TO DO?

So will the critical infrastructure and cyber security initiatives in Part IV of the BTBAP[45] help accelerate joint activities between Canada and the United States? Not likely in any significant way. In fact, it is surprising that after almost ten years of cooperation between Canada and the United States on these issues, there are still so few specific details (the section dealing with critical infrastructure and cyber security contains fewer concrete, new commitments than almost any other component of the plan).[46]

Let's have a look at some of the key elements in the plan that the two governments have committed themselves to:

---

42. ORG. OF AM. STATES, http://www.oas.org/en/default.asp (last visited Dec. 16, 2012).

43. GRAHAM, *supra* note 6, at 19.

44. *Id.* at 20.

45. *See* BTB, *supra* note 1, at 23-25.

46. *See id.*

> "Execute programs and develop joint products to enhance cross-border critical infrastructure protection and resilience."[47]

This is largely a promise to make good on the CUSCI announced back in 2010.[48] Had this commitment been fleshed out in greater detail in the BTB and included clear deadlines and deliverables, it might have signaled a renewed commitment to action. But it is not.

> "[C]onduct a regional resilience assessment program (RRAP) for the Maine-New Brunswick region . . . ."[49]

While regional initiatives can contribute significantly to enhanced Canada-United States resilience, there are higher priority issues that need to be addressed, first at the level of bi-national leads.

> "[C]reate binational mechanisms for joint risk analysis, which will share information and develop joint analytic products."[50]

While this activity holds promise, such mechanisms and products already exist. Is some new, more intensive effort being proposed?

> "[E]nhance our already strong bilateral cyber security cooperation to better protect vital government and critical digital infrastructure and increase both countries' ability to respond jointly and effectively to cyber incidents. This will be achieved through joint projects and operational efforts, including joint briefings with the private sector and other stakeholders and the enhancement of real-time information sharing between operation centres."[51]

It is not at all clear what this commits governments to in specific terms.

> "Expand joint leadership on international cyber security efforts"[52] and "strengthen cooperation on international cyber security and Internet governance issues . . . ."[53]

Again, while this is a laudatory objective, it is a vague commitment lacking in specifics.

---

47. *Id.* at 23.

48. See CUSCI, *supra* note 2.

49. BTB, *supra* note 1, at 23.

50. *Id.*

51. *Id.*

52. *Id.* at 24.

53. *Id.*

In summary, there is little in the way of new, meaningful joint activity on critical infrastructure and cyber security in the BTB.

SO WHERE SHOULD WE GO FROM HERE?

In order to sustain joint efforts, Canada and the United States must immediately develop an ambitious, comprehensive, bi-national plan, setting out in detail how the two nations will work together to prepare for, respond to, and recover from cyber and critical infrastructure threats and disruptions. This should be fleshed out over the coming six-to-twelve months and finalized in detail within the next two years at the latest. To be effective, the plan should include both cyber security (cyber systems and networks) and critical infrastructure (especially cyber-supported critical infrastructures).[54] It could perhaps take the form of a single plan with two annexes. This work should be closely coordinated with the law enforcement[55] and trade[56] sections in the BTBAP.

This initiative will require dedicated resources and a recognition that participants will have to devote significant time outside of their day-to-day responsibilities to complete this work; there is no way around this. Governments are either committed to producing results or they are not. It should include ambitious, explicit actions, establish accountabilities, include expected results and rigorous timelines for each action item, including a clear designation of which individuals or agencies will be leading and supporting the effort, and what they are each expected to deliver and by when. There should be robust reporting requirements and mechanisms for tracking results.

The plan should focus on a number of key priorities,[57] each of which should set out bold objectives and deliverables. The plan should be reviewed semi-annually by a small, bi-national steering group of senior officials, and reviewed annually by Ministers/Cabinet Secretaries. A report to the general public and stakeholders should be made following each annual review. Possible priorities might include any number of the following:

54. Both issues, for the most part, are currently dealt with in isolation by both governments. *See, e.g.*, CUSCI, *supra* note 2 (discussing critical infrastructure but making no specific mention of cyber security).

55. *See* BTB, *supra* note 1, at 21.

56. *See id.* at 11-19.

57. Such priorities could be identified jointly by a small group of senior officials from both countries in a one day facilitated retreat using simple SWOT (Strengths/Weaknesses/Opportunities/Threats) analysis. *See, e.g.*, Tim Berry, *How to Perform SWOT Analysis*, BPLANS.COM, http://articles.bplans.com/business/how-to-perform-swot-analysis/116 (last visited Dec. 16, 2012).

1. Develop a systematic, long-term agreement or protocol between Canada and the United States for identifying, sharing, and protecting cyber security and critical infrastructure information, and set specific modalities and mechanisms for doing so.[58]

2. Prepare a mutual agreement or protocol setting out clear roles and responsibilities of departments and agencies in each country involved in joint cyber security and critical infrastructure activities. Clarify, in particular, the roles of public safety/security departments, defence border, law enforcement and intelligence agencies. Sort out the complex jumble of roles and competing interests. Designate lead agencies for various activities.

3. Develop a detailed concept of operations (CONOPS)[59] setting out rules of engagement for joint operational activities.[60]

---

58. A good beginning already exists. *See* CUSCI, *supra* note 2 (committing Canada and the United States to coordinate alerts and certain information products). More needs to be done, however, to determine: (1) information that is available; (2) the constraints that exist in sharing different types of information across the border and with the private sector; and (3) the mechanisms and procedures that need to be put in place. There are numerous examples of such detailed information-sharing agreements in other spheres, such as immigration. *See, e.g.*, Press Release, Off. of the Spokesperson, U.S. Dep't of State, U.S.-Canada Visa and Immigration Information-Sharing Agreement (Dec. 14, 2012), *available at* http://www.state.gov/r/pa/prs/ps/2012/12/202065.htm.

59. A concept of operations (CONOPS) is a description of how a set of capabilities should be employed to achieve desired objectives or a desired end state. It should describe processes to be followed and a clear methodology to realize the goals and objectives of the system. In general, it will include the following:

    1. Statement of the goals and objectives of the system;

    2. Strategies, tactics, policies, and constraints affecting the system;

    3. Organizations, activities, and interactions among participants and stakeholders;

    4. Clear statement of responsibilities and authorities delegated;

    5. Specific operational processes for fielding the system; and

    6. Processes for initiating, developing, maintaining, and retiring the system.

    See, e.g., WMO, STANDARD OUTLINE FOR DOCUMENTATION OF GOOD PRACTICES IN MULTI-HAZARD EARLY WARNING SYSTEMS 2 (2009), *available at* http://www.wmo.int/pages/prog/drr/events/MHEWS-II/Documents/Doc-5-FINALEWSDocumentationTemplate.pdf.

The multi-faceted nature of critical infrastructure systems points to the urgent need for a clearly defined modus operandi involving many stakeholders interacting across borders in complex ways, and yet operating as an integrated system. The CONOPS should govern operational linkages between Public Safety Canada and Department of Homeland Security operations centres, the ("CERTS"),[61] law enforcement, defence and intelligence agencies, private sector players, and states and provinces. It could also include provisions for staff exchanges, joint training, and exercises. Governments should set a bold objective to achieve this, --for example: "by 2015 the United States and Canada will achieve full joint operating capabilities in cyber security as set out in a comprehensive joint concept of operations, to be completed by June 2014. The concept of operations will include the following specific elements ('xyz'), and will take the form of a formal agreement between both parties to be signed at the level of Cabinet Secretary/Minister," etc.

4. Create a robust joint analytical capability dedicated to policy analysis in priority areas such as legal frameworks, regulatory options, standards development, identity management, personal privacy, and data protection. Develop a framework for joint research and development priorities. This could perhaps be done under the auspices of the existing Agreement Between the Government of Canada and the Government of the United States of America for Cooperation in Science and Technology for Critical Infrastructure Protection and Border Security.[62]

5. Jointly develop a private sector engagement strategy setting out a formal consultative process with sectors, resulting in a clarification of roles and expectations for private sector involvement in cyber security and infrastructure protection. This is not an optional activity. The private sector must be drawn in from the beginning.

60. Joint operational activities could include, both bilateral and multilateral watch and warning efforts; intrusion detection; incident management; forensics; investigations and response; threat assessment; risk analysis; training and staff exchanges; joint exercises; and, information protection and dissemination.

61. Otherwise known as "Computer Emergency Response Centers."

62. *See* Science and Technology Agreement, *supra* note 32.

6. Develop a paper setting out options for possible joint "Five Eyes,"[63] European Union, NATO, and other multilateral engagements.

7. Undertake an immediate stock-taking of cyber security standards by sector and require critical infrastructure sectors to prepare voluntary or mandatory cyber security standards within a set timeframe.

8.Finally, and perhaps most importantly, identify senior champions to steer and drive the collaboration process and to hold people accountable for results.

ISSUES FOR CONSIDERATION

1. Are the goals in the BTBAP detailed and challenging enough to significantly deepen and intensify Canada-United States cooperation on these issues? What key, concrete deliverables are missing?

2. Are these goals attainable within a reasonable timeframe, given the differences in governance, legislation, policy, and capacity that exist between Canada and the United States in many of these areas?

3. Does each nation have its own house sufficiently in order to allow it to commit the energy and resources necessary to achieve these joint goals? Will domestic considerations or simply lack of interest prevent the United States from devoting serious attention to bilateral activities with Canada? Note for example the intense, ongoing debate in the U.S. over proposed legislative/executive action related to cyber security standards. Do bilateral relations stand a chance of succeeding in such an environment?

4. Timing is everything. Canada, in particular, should use the hiatus in American activity resulting from pending decisions on legislative mandates to further refine its positions on issues like privacy, voluntary versus mandatory standards, and international standards development. This will be crucial if joint Canada-United States activities are to keep pace with the sizzling rate of international developments.

5. What is the ultimate end game of cooperation for the United States and for Canada? Is it policy, legislative, and operational

63. "Five Eyes" is a term used to describe the intelligence alliance between the United States, Canada, Australia, New Zealand, and the United Kingdom. *See, e.g.*, Kady O'Malley, *Do the "Five Eyes" Watch Each Other?*, CBC NEWS (Oct. 10, 2012), http://www.cbc.ca/news/politics/inside-politics-blog/2012/10/from-the-order-paper-question-archives-do-the-five-eyes-watch-each-other.html.

convergence, or is it something less than that? What are the alternatives?

6. Is there the political will, not just in Canada and the United States, but internationally, to address the contentious issues of data protection and personal privacy rights?[64] This is particularly relevant in light of strong reactions in Canada to the provisions of the Canadian Government's online surveillance Bill C-30[65] and reactions immediately following September 11 to the privacy implications of the "Patriot Act" in the United States.[66] It is also reflected in the recent heated debate in the United States over an expanded domestic cyber security role for the National Security Agency,[67] in the European Union's plans to bolster data protection rights for individuals,[68] and in the public debate over data protection under cloud computing.[69]

---

64. *See, e.g.*, Rick Mercer, *Rick's Rant–Online Privacy*, CBC PLAYER (Feb. 21, 2012), http://www.cbc.ca/player/Shows/Shows/The+Rick+Mercer+Report/Rick%27s+Rants/ID/2200235120/ (last visited Dec. 16, 2012) (depicting a "slightly over the top" discussion that sums up the reactions of many Canadians about intrusions into personal privacy).

65. *See, e.g.*, Heather Mallick, Op-Ed., *Conservative Bill C-30 Will Let Police Spy on Canadians Online*, TORONTO STAR (Feb. 14, 2012), http://www.thestar.com/opinion/editorialopinion/article/1131446--conservative-bill-c-30-will-let-police-spy-on-canadians-online.

66. *See, e.g.*, *Patriot Act Seen as Threat to Canadians' Privacy*, CBC NEWS (June 20, 2006, 2:10 PM), http://www.cbc.ca/news/canada/story/2006/06/20/privacy-report.html.

67. *See, e.g.*, Mark M. Jaycox, *Why the NSA Can't Be Trusted to Run U.S. Cybersecurity Programs*, ELEC. FRONTIER FOUND. (July 30, 2012), https://www.eff.org/deeplinks/2012/07/why-nsa-cant-be-trusted-run-us-cybersecurity-programs.

68. *See, e.g.*, Press Release, European Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of their Data and to Cut Costs for Businesses (Jan. 25, 2012), *available at* http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en.

69. *See, e.g.*, Michael Chertoff, Op-Ed., *Cloud Computing and the Looming Global Privacy Battle*, WASH. POST (Feb. 9, 2012), http://articles.washingtonpost.com/2012-02-09/opinions/35444049_1_data-privacy-cloud-storage-data-protection ("A set of global rules will be difficult to achieve. International structures are notoriously cumbersome and slow moving; this is a particular challenge in the context of quickly developing cloud technology. And international organizations' governance structures are often universally inclusive, which means that countries with little interest in Internet freedom or accessibility may have a disproportionate influence on the rules adopted. . . . The alternative, however, is equally problematic. If development of privacy rules and regulations is left to individual countries, one of three scenarios is likely to result: Heralded by E.U. actions, more fragmented regulation may emerge as non-European countries try to impose their

7. Is the Agreement Between the Government of the United States of America and the Government of Canada on Emergency Management Cooperation,[70] with its relatively recent involvement and lack of bench strength on critical infrastructure and cyber security issues, really the vehicle best suited to serve as the "cornerstone" of these joint efforts?

8.How effectively does this plan address the important question of cooperation between the United States and Canada at a global level?[71] What are the respective roles of bilateral relations with trusted partners, like-minded groups like "Five Eyes", the European Union, and various other multilateral organizations? Will Canada and the United States attempt to arrive at common positions on the development of international standards and protocols in these areas?[72] At a minimum, will they undertake to consult or advise each other prior to taking major new positions in multilateral forums?

9.Finally, the BTB commits the Canadian and American Governments to enhancing the resiliency of shared critical and cyber infrastructure. But are the two nations still placing too much emphasis on threats and vulnerabilities and not enough on how we

---

own privacy views on an unruly network. . . . Another possibility is a rush to the bottom as countries compete to attract commercial cloud services by minimizing privacy protections. . . . The most likely result, however, is a privacy clash as the United States and the European Union compete to impose their will. This is the worst possible outcome, pitting natural allies against each other. U.S. diplomacy should urgently focus on dissuading Europe from unilateral action while developing a comprehensive 'Western' approach to cloud privacy.").

70. Agreement on Emergency Management Cooperation, U.S.-Can., Dec. 12, 2008, T.I.A.S. No. 2010-0071.

71. *See generally, e.g.*, U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-10-606, CYBERSPACE: UNITED STATES FACES CHALLENGES IN ADDRESSING GLOBAL CYBER SECURITY AND GOVERNANCE (2010) (discussing key international organizations involved in cyber security and the challenges that the United States faces in the area of international cyber security arrangements; yet, no reference is made to bilateral arrangements, such as with Canada).

72. Canada has had, and continues to have, a close strategic alliance with the other "Five Eyes" nations—United States, United Kingdom, Australia, and New Zealand—on signals intelligence, dating back to the 1940s. It is therefore somewhat surprising that recent collaboration between the United States, the United Kingdom, and Australia on a trilateral initiative to fund new research and development for improved cyber security has not included Canada. *See, e.g.*, Press Release, Off. of the Press Sec'y, The White House, Joint Fact Sheet: U.S.-UK Progress Towards a Freer and More Secure Cyberspace (Mar. 14, 2012), *available at* http://www.uspolicy.be/headline/white-house-us-uk-cybersecurity-partnership.

deal with the actual *consequences* of a major failure or attack? What specific activities do they have in mind for developing more resilient joint response and recovery capabilities?

In conclusion, while the commitments made in the BTBAP may ultimately lead in the right direction, they are a rather timid collection of ad hoc, ongoing activities that will do little to galvanize players on either side of the border.

Canada and the United States need to do some serious soul-searching—and quickly—about the desired end state and specific joint actions they will commit themselves to in the areas of Cyber security and critical infrastructure protection if they are to take full advantage of the important window of opportunity the BTBAP provides.

POSTSCRIPT

This article was written in Fall 2012, at a time when efforts to address these issues appeared to be floundering on both sides of the border. Efforts to date had been largely perfunctory and half-hearted. As this goes to print, however, governments and legislators in both countries seem seized with the importance of making these issues *domestic* policy priorities. Only time will tell, however, whether governments are serious about tackling them as important *bilateral* priorities.