Now for the Hard Part: Renewing Regional Cooperation on Critical Infrastructure Security and Resilience

Brian Bow

Joint Publication with the Canada Institute and the Canadian International Council

September 2014

Now for the Hard Part: Renewing Regional Cooperation on Critical Infrastructure Security and Resilience

Brian Bow

Critical infrastructure security and resilience (CISR) has been one of the core priorities for North American regional security cooperation since 9/11.[1] More than a dozen years later, extensive consultation within and between the United States, Canada, and Mexico has finally begun to generate some tangible results, including ongoing information-sharing, the development of cross-border emergency response procedures, and joint exercises. These have been touted by some as signs of meaningful progress, but the nature of the results says more about the weakness of the regional effort than its strength. To the extent that concrete steps have been taken, the focus has been on anticipating and responding to infrastructure crises, rather than preventing them through deeper protection measures or minimizing their impact through the elimination of points of vulnerability and the creation of systemic redundancies. Without a renewed political commitment to long-range consultation, planning, and spending, the regional CISR agenda will stall, wasting costly investments already made, leaving obvious vulnerabilities unaddressed, and ultimately putting lives at risk.

Recommendations:

1. As an extension of ongoing United States-Canada and United States-Mexico bilateral talks, the Department of Homeland Security (DHS), in combination with Public Safety Canada (PS) and Centro de Investigación y Seguridad Nacional (CISEN), should convene a trilateral expert panel to develop a strategic framework for long-term CISR planning in North America, mapping out a set of goals, timetables, and spending commitments.

2. DHS, PS, and CISEN should organize a series of high-profile expert presentations aimed at legislators, media, and academics, on cutting-edge CISR challenges and strategies, including recent technological developments, alignments and discrepancies in national infrastructure and CISR plans, and the evolution of national legislation on public-private partnerships on CISR.

3. DHS, PS, and CISEN should re-engage with private sector stakeholders to promote a reconceptualization of CISR as an important aspect of corporate social responsibility

[1] This set of issues has gone by many names in recent years, including critical infrastructure protection (CIP) and security of critical infrastructure and key resources (CIKR). These variations have subtle but important framing effects on the policy debate, but the underlying set of relevant policy challenges is essentially the same.

(CSR) for North American business. It is time to start pushing public-private engagement on CISR beyond relationship-building and information-sharing, by negotiating new planning and spending commitments to create critical infrastructure systems that are harder to disrupt, more adaptable, and quicker to recover.

CISR as a political and diplomatic challenge

Even before NAFTA and 9/11, the United States, Canada, and Mexico all recognized the need to secure critical infrastructure and to collaborate with their continental neighbors in doing so. New technologies and new rules governing trade and investment spurred a late-twentieth century transition into a new knowledge economy, characterized by urbanization, automation, and new emphasis on lean manufacturing, services, and finance. This new economy created new opportunities for efficiency and growth, but it also created new societal and economic vulnerabilities, based on its dependence on physical and cyber infrastructures that are massive in scale, incredibly complex, and increasingly "brittle" in the face of various potential disruptions.

NAFTA encouraged the growth of continental-scale intra-firm trade and complex supply chains, often based on just-in-time production and distribution systems. These new investments and new management structures created real interdependencies between the three NAFTA partners: if one grew, the others would benefit; but if one suffered a significant disruption of critical infrastructure, the others would likely suffer as well. 9/11 gave new political momentum to national efforts to secure critical infrastructure and new attention to mutual vulnerabilities, but it focused the agenda relatively narrowly on the "protection" of national infrastructure against deliberate attacks and on border infrastructure at the expense of broader continental-scale systems. The Northeast Blackout of August 2003 and Hurricane Katrina two years later shifted attention back toward more mundane, "pre-9/11" threats like natural disasters, computer control failures, human operator error, and physical degeneration due to lack of maintenance or upgrades. Thus the agenda was reframed from "protection" to "security and resilience," to encompass a system's capacity to withstand an attack or other crisis (robustness), the capacity to sustain vital services during a crisis through the availability of alternative mechanisms (redundancy), the potential to mobilize necessary resources to mitigate the effects of a crisis (resourcefulness), and the speed with which baseline services can be restored through emergency response (rapidity).[2]

[2] This "four Rs" conceptualization of CISR is developed in T.D. O'Rourke, "Critical Infrastructure, Interdependencies, and Resilience," *The Bridge: National Academy of Engineering* 37 (Spring 2007).

2001-09: An ambitious regional agenda, but slow progress in national efforts

The three North American partners signaled their commitment to CISR after 9/11 by empowering new national agencies—Department of Homeland Security in the United States, Public Safety in Canada,[3] and Centro de Investigación y Seguridad Nacional (CISEN) in Mexico—to manage inter-agency coordination and keep these complex agendas on track. The United States renewed bilateral talks with each of its neighbors through the 2002 Smart Border Accords; this agenda was again taken up, on a trilateral basis, through the 2005 Security and Prosperity Partnership (SPP). After the SPP was discontinued in 2009, the United States renewed CISR talks with Canada and Mexico on a bilateral basis: US-Canada coordination was pursued through the Beyond the Border (BTB) initiative, launched in 2010; US-Mexico coordination has been carried out through informal contacts established under the Smart Border agreements and the SPP, and as a marginal consideration in bilateral talks like the 21st Century Border (21CB) initiative.

Apart from the switching back and forth between bilateral and trilateral diplomacy, the basic format and approach for CISR collaboration has been essentially the same over the last 20 years, featuring ongoing, informal consultation between bureaucrats and technical experts, organized into multi-agency working groups, focused on coordinating policies through reciprocal executive commitments, rather than the negotiation of formal treaty commitments. Under the Smart Border agreements and the SPP, the substantive focus was on working out a shared concept of critical infrastructure, compiling and sharing information about the existing critical infrastructures in each of the three countries, and discussing "best practices" in the sharing and updating of information, with some preparatory planning for joint emergency response. In practice, most of the coordination on emergency response issues was concerned with removing obvious obstacles to cross-border assistance in an emergency, such as sharing and updating of emergency contacts, basic procedures for emergency notification, and changes to cumbersome

The basic format and approach for CISR collaboration has been essentially the same over the last 20 years, featuring ongoing, informal consultation between bureaucrats and technical experts, organized into multi-agency working groups.

[3] Public Safety Canada was originally launched in 2003 as Public Safety and Emergency Preparedness Canada (PSEPC).

legislative rules and bureaucratic procedures governing cross-border contacts and emergency border-crossing by first responders.[4] A few more tangible results were achieved under the SPP, including risk-assessment studies and emergency response exercises. Leading proponents of the SPP argued that this was important progress on the road to more effectively collaborative CISR, but critics dismissed it as little more than "making plans to make plans."

By the time the SPP was discontinued, post-9/11 CISR collaboration was starting to show results, at least within the bilateral US-Canada context. Though some were unsatisfied with the official working definitions, there was in practice an emergent consensus around the basic meaning of "critical infrastructure"[5] and on a relatively broad framing of goals around "security" and "resilience." Equally importantly, the long, sometimes-difficult process of building relationships among agencies within each country and between countries was well under way, and a new transnational network of officials and technical experts could be seen coalescing around a fairly clear-cut series of recurring meetings, exchanges, and exercises.[6] A few, more ambitious sector- or region-specific initiatives had been launched during and after the SPP, such as the pilot-program regional resilience assessment project for Maine and New Brunswick and US-Mexico plans for joint emergency response to environmental crises in the border area. But for the most part these represent only slightly more "tangible" versions of the basic network-building process observed more generally.

2009-: Accelerated national efforts, fragmentation of regional coordination

Once the core cross-border networks were established, however, and a common language had been worked out, political and bureaucratic energy shifted from cross-border consultation toward more determined efforts to develop concrete national strategies. After 9/11, presidential directive HSPD-7 called for the development of a US National Infrastructure Protection Plan (NIPP), which was first rolled out in 2003. Subsequent iterations of the NIPP were launched in 2009 and 2013, each with a slightly-sharper definition of critical infrastructure and more detailed plans for the identification and prioritization of CISR efforts.[7] Because the

[4] Security and Prosperity Partnership, "Security Priorities," August 2006. [http://www.spp-psp.gc.ca/eic/site/spp-psp.nsf/vwapj/security-2006-Aug-10.pdf/$file/security-2006-Aug-10.pdf] See also DHS, "Compendium of US-Canada Emergency Management Assistance Mechanisms," June 2012. [http://www.dhs.gov/xlibrary/assets/policy/btb-compendium-of-us-canada-emergency-management-assistance-mechanisms.pdf]

[5] See, for example, the discussion of critical infrastructure protection in the North American Plan for Avian and Pandemic Influenza, finalized under the SPP in August 2007. [http://2001-2009.state.gov/documents/organization/91309.pdf]

[6] White House, "Beyond the Border Implementation Report: December 2013," December 19, 2013. [http://www.whitehouse.gov/sites/default/files/docs/btb-canada-us-final_-_dec19.pdf]

[7] DHS, "National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience," December 23, 2013.

nature of the challenges varies significantly across different sectors, the NIPP agenda was broken up into 17 different sector-specific plans (SSPs), and then expanded to 18 with the inclusion of critical manufacturing. Within some of these sectors—e.g., nuclear power, banking and finance—sector-specific guidelines and plans were quickly worked out, not only for the sharing of technical information and best practices, but even relatively clear-cut plans for emergency response and restoration of service after a disruption. In others—e.g., transportation and telecommunications—progress has been minimal at best, with participants struggling to agree on sector membership, working definitions of critical infrastructure, and general principles to guide routine information sharing.[8]

With the coalescence of the second US NIPP in 2008-09, and the concurrent unraveling of the SPP process, Canadian and Mexican policymakers shifted into a more reactive approach to CISR, focusing on keeping track of developments in Washington, and adapting their own processes and outcomes to "fit" with evolving US standards and practices. Canada developed its own national plan, at the same time that it was negotiating a binational collaboration framework with the United States; the National Strategy for Critical Infrastructure was unveiled in May 2010, and the US-Canada Action Plan for Critical Infrastructure in July of that year.[9] The Harper government also unveiled national plans for cybersecurity in 2010 and for counter-terrorism in 2012. Canada's overall infrastructure development got a boost from 2009 stimulus spending, and the Harper government has committed to keep up spending

Mexico, not surprisingly, lags behind the United States and Canada on CISR policy, and U.S.-Mexico bilateral coordination is much less extensive than that between the United States and Canada. However there is some confidence that Mexico can start to catch up relatively quickly, based on the Peña government's commitment to infrastructure development and the availability of the U.S.-Canada experience as a model for further U.S.-Mexico bilateral coordination.

[http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf]

[8] GAO-07-39, "Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sector Characteristics," November 15, 2006. [http://www.gao.gov/products/GAO-07-39]

[9] Public Safety Canada, "National Strategy for Critical Infrastructure," May 28, 2010. [http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-eng.aspx] The Canadian national strategy was recently updated for 2014-17. DHS, "US-Canada Action Plan for Critical Infrastructure," July 2010. [http://www.dhs.gov/xlibrary/assets/ip_canada_us_action_plan.pdf]

through its new, 10-year Building Canada plan. In May 2013, the United States and Canada launched a binational Border Infrastructure Investment Plan, with a commitment to share spending plans and push ahead more aggressively with previously-identified border infrastructure projects, including plans to upgrade a number of smaller, out-of-the-way crossings. However, there are still significant gaps in Canada between federal and subfederal governments and between public and private actors on CISR issues, and even the relatively ambitious new Action Plan does not go much beyond sharing of information and best practices.

Mexico, not surprisingly, lags behind the United States and Canada on CISR policy, and US-Mexico bilateral coordination is much less extensive than that between the United States and Canada. However there is some confidence that Mexico can start to catch up relatively quickly, based on the Peña government's commitment to infrastructure development and the availability of the US-Canada experience as a model for further US-Mexico bilateral coordination. US and Mexican officials have been talking about CISR issues since the Smart Border Accord, but progress in relationship-building and information-sharing has been slow. And most of the conversation about bilateral coordination on these issues has been very narrowly focused on the improvement of infrastructure directly connected to border crossings.[10] Nevertheless, there is clearly political momentum behind infrastructure development in Mexico now, a willingness to undertake politically-risky market reforms in sensitive sectors like oil and gas, electricity, transportation, and telecommunications, and an interest in integrating CISR into national planning.

There is clearly political momentum behind infrastructure development in Mexico now, a willingness to undertake politically-risky market reforms in sensitive sectors like oil and gas, electricity, transportation, and telecommunications.

The form and purposes of regional CISR cooperation today are very different than most advocates envisioned after 9/11. The Smart Border agreements and the SPP pledged to develop threat assessments and make policy changes to address the most urgent vulnerabilities, but we seem now to be settling for talking about what kinds of crises might take place and about how to clean up the mess afterward. The United States is struggling to develop its own national strategies for CISR and for infrastructure development more generally. It engages with Canada and Mexico mainly to follow through on border infrastructure projects that were planned years

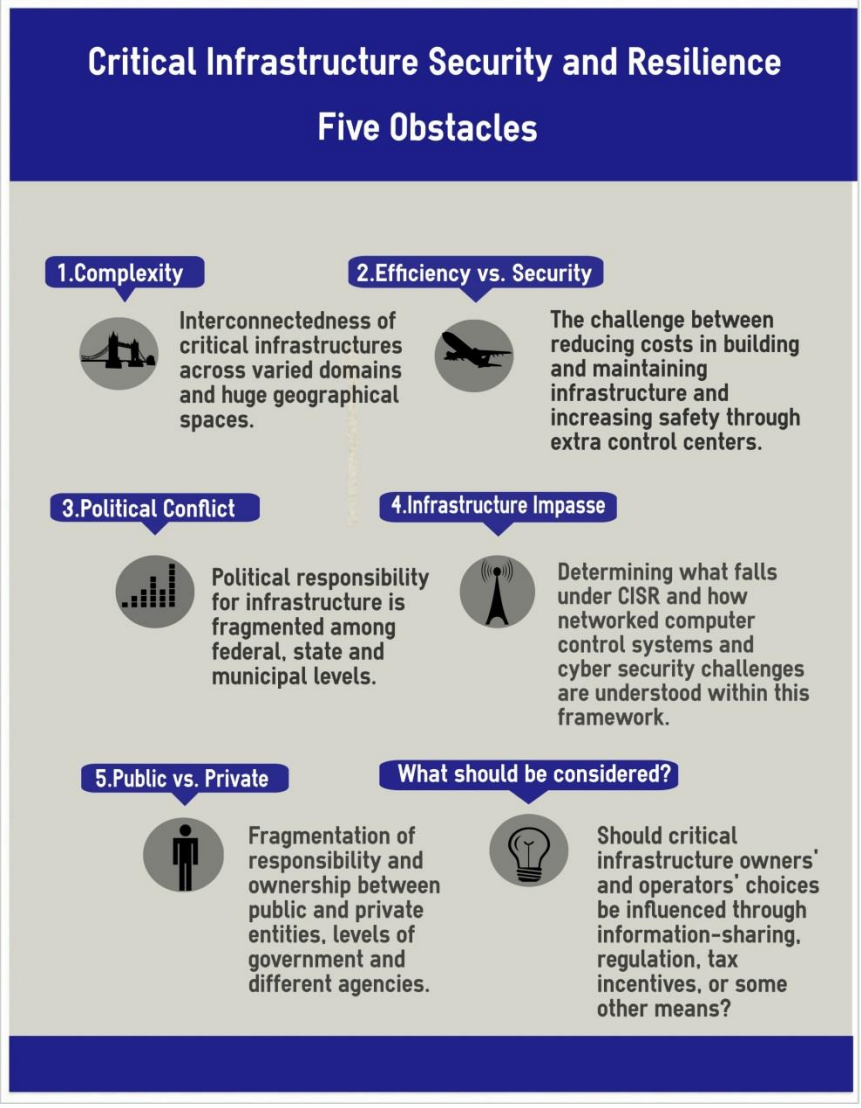
[10] DHS, "21st Century Border Management 2013 Progress Report," n.d. [http://www.dhs.gov/sites/default/files/publications/press/21cb-progress-report-2013.pdf]

ago. The private sector has shown a willingness to engage with government CISR planners, but that support is very tentative, shying away not only from any hint of new regulation, but even from many forms of basic information-sharing. Collection of information is patchy, threat assessments are few and far between, and—most importantly—virtually nothing is being done to encourage critical infrastructure owners and operators to make significant improvements to security and resilience (i.e., real-time monitoring, physical and cyber safeguards, system redundancies). The result is that the regional CISR agenda has lost momentum, and given up any sense of strategic ambition.

Five obstacles

It is important to understand that CISR is an inherently difficult public policy problem and that most of the obstacles to effective CISR coordination are domestic and political, rather than diplomatic. The general slow-down of regional cooperation after the collapse of the SPP process has played a part in the loss of momentum behind CISR cooperation, but only a minor part.

Figure 1. Five Obstacles to Critical Infrastructure Security and Resilience



Complexity

The core difficulty with CISR is the scale and complexity of critical infrastructure in the contemporary economy and the interconnectedness of critical infrastructures across varied domains and huge geographical spaces. The problems associated with this kind of interconnectedness have been further compounded by the rapid proliferation of increasingly-autonomous computer control systems designed to monitor, adjust, and shut down factory production lines, heating and cooling systems, electrical grids, traffic control systems, and other complex systems. The 2003 Northeast Blackout event illustrated the nature and extent of the challenge, when a software fault at one power company's control center triggered a cascade of shutdowns across multiple electrical distribution networks, spreading from Ohio to New England and up into Ontario, ultimately affecting more than 50 million people. Power failures disabled airport inspections, train guidance systems, gas stations, water pumps, and cell phone towers, paralyzing travel and communications and contributing to at least 11 deaths.

The core difficulty with CISR is the scale and complexity of critical infrastructure in the contemporary economy and the interconnectedness of critical infrastructure across varied domains and huge geographical spaces.

Efficiency versus security

There is, moreover, a built-in tension in the design of infrastructure systems, between efficiency and resilience. Reducing the enormous costs associated with building and maintaining infrastructure—whether in the private sector or public—usually involves massively increasing scale, automating operations, reducing the number of control stations, and minimizing regulatory paperwork and oversight. These economic imperatives are often directly contradictory to the pursuit of resilience—that is, a system's capacity to absorb stress in a crisis and bounce back, ensuring the continuation of vital services or restoring them quickly after a disruption. One of the surest ways to increase resilience is to create redundancies in the system by building "extra" control centers, power stations, pipelines, pumps, or emergency response crews. Redundancy may be appealing to a safety engineer, but for a manager, it is just another word for inefficiency and mismanagement. This is a problem for publicly-owned and operated utilities seeking to reduce costs in an era of fiscal restraint, but it is even more daunting when it comes to the private sector—and about 85 percent of critical infrastructure in the United States is privately owned and operated. Furthermore, because CISR planning necessarily involves collecting information on what critical infrastructure exists and where it might be vulnerable, government engagement with private sector operators has run up against the latter's

legitimate concerns about protecting sensitive and proprietary information. The Obama administration attempted to address these concerns in the 2013 NIPP, but early indications suggest that private sector concerns about this kind of information-sharing are still a significant obstacle to effective public-private collaboration.[11]

Infrastructure impasse

Even where there is a rough consensus about what critical infrastructure is and the need to do something about it, the agenda is further complicated by the fact that CISR cannot be effectively separated from the broader problem of infrastructure development more generally, or—thanks to the proliferation of networked computer control systems—from the "new" and not-yet-well-understood challenges of cybersecurity. The attachment to infrastructure more broadly is a huge political anchor for CISR because of the intense controversies surrounding fiscal policy and the intensifying polarization of politics, particularly in the United States. The connection to cybersecurity, on the other hand, may help to attract attention and support for CISR, but its implications are still somewhat ambiguous, at least partly because there is still so much technical and political uncertainty surrounding cybersecurity.

The agenda is further complicated by the fact that CISR cannot be effectively separated from the broader problem of infrastructure development more generally, or from the "new" and not-yet-well-understood challenges of cybersecurity.

Political conflict

These issues are further complicated by the fact that political responsibility for infrastructure is fragmented, both horizontally among multiple agencies at the federal level and vertically among the federal, subfederal (i.e., states and provinces), and municipal levels. Policymaking by any of these types of actors can be, and in practice frequently has been, effectively blocked by the others. And the negotiation of some kind of workable division of responsibility among the various actors and levels has been made almost impossible in recent years by the all-out struggle among these players over the raising and disbursement of tax revenues.

[11] GAO-14-464T, "Critical Infrastructure Protection: Observations on Key Factors in DHS's Implementation of Its Partnership Approach," March 26, 2014. [http://www.gao.gov/products/gao-14-464t]

Public versus private

The fragmentation of responsibility, between public and private players, and between different agencies and levels of government, further complicates an already difficult technical debate over how CISR might be effectively pursued through public policy. Where there are trade-offs to be made between efficiency and security/resilience, how are those values to be weighed against one another? Who decides what standards and practices are to be followed? Who monitors compliance and enforces the rules? Who pays the costs associated with compliance-monitoring and enforcement? Should critical infrastructure owners' and operators' choices be influenced through information-sharing, regulation, tax incentives, or some other means? So far this "debate" has been mostly left implicit, at least in part because government planners have been reluctant to risk alienating private sector stakeholders.

Windows of opportunity

Given the complexity of these issues and the inherent political tensions surrounding various policy tools that might be employed to pursue CISR, it is probably not surprising that more has not yet been accomplished at the national or regional levels. Even "making plans to make plans" is a difficult, time-consuming process. New personal relationships have been built, lines of communication are open, and some of the most obvious potential obstacles to emergency cooperation have been identified and dragged out of the way. Relevant private sector players have been willing to engage with the process, at least in some sectors. So the development of new national programs and bilateral framework agreements on CISR cooperation do represent significant political and diplomatic achievements. If, however, we were to rest on these laurels, then most of the hard work of CISR will have been left undone. Based on the coordination that has taken place so far or is in train now, we might develop the means to identify a critical infrastructure failure with regional implications, and perhaps also to develop an ad hoc coordinated response to a future critical infrastructure emergency. But without substantial new investments, we will not have the means to anticipate such an emergency, design and build systems that could prevent or mitigate it, or actually carry out a coordinated emergency response.

But without substantial new investments, we will not have the means to anticipate such an emergency, design and build systems that could prevent or mitigate it, or actually carry out a coordinated emergency response.

New momentum for infrastructure-building?

There are, on the other hand, at least two reasons to think that now is the time to push ahead on these issues, though not necessarily to be optimistic about a political breakthrough. First, there is (still) significant interest in infrastructure investment more generally, in all three countries, though perhaps less than it sometimes appears. All three governments made infrastructure projects a priority in their stimulus spending after the 2008 financial crisis, and particular attention was given to critical infrastructure like highways, bridges, water systems, and flood control.[12] And each has recently rolled out a new national infrastructure plan that promises to keep up spending levels on infrastructure renewal.

Canada has a lot of work to do in repairing and upgrading national infrastructure; the Harper government has committed itself to address the problem through its Building Canada program, first launched in 2010. A New Building Canada Plan was launched in February 2014, with $50 million in federal funding to support infrastructure projects undertaken by provincial and municipal governments.[13] Mexico has been making significant strides to rapidly upgrade and expand its own infrastructure over the last decade. President Calderón produced an ambitious, $230 billion infrastructure-building plan for 2007-12, and Peña topped it with a $590 billion plan for 2014-18.[14]

The United States is the laggard in terms of national infrastructure commitments, but not for lack of trying, at least on the part of the White House. The Obama administration is clearly committed to infrastructure-building as a means to both short-term economic stimulus and long-term competitiveness, but has been repeatedly stymied by Congress, as part of the much broader partisan polarization in recent years. Obama's newest legislative proposal, the GROW AMERICA Act[15] unveiled in April, would provide $300 billion for various infrastructure projects,

---

[12] United States, White House, "Opportunity for All: Building a 21st Century Infrastructure," April 29, 2014. [http://www.whitehouse.gov/sites/default/files/omb/budget/fy2015/assets/fact_sheets/building-a-21st-century-infrastructure.pdf] Infrastructure Canada, "New Building Canada Plan," March 28, 2014. [http://www.infrastructure.gc.ca/plan/nbcp-npcc-eng.html] Mexico, Office of the President, "National Infrastructure Program, 2014-18," April 30, 2014. [http://en.presidencia.gob.mx/national-infrastructure-program-2014-2018/]

[13] The overall amount of this commitment is less than it appears to be, as it is stretched over a 10-year period. Most of the promised funding does not come into play for several years to avoid undermining the government's pledge to balance the budget.

[14] Anthony Harrup, "Mexican Government Boosts Infrastructure Investment Plan," *Wall Street Journal*, April 28, 2014. [http://online.wsj.com/news/articles/SB10001424052702304163604579530131171053254] These huge numbers are less impressive than they might first appear, since both figures are mostly driven by massive investments in oil and gas infrastructure, and Peña's includes housing, health, and tourism ventures not normally counted in national infrastructure plans.

[15] The acronym stands for Generating Renewal, Opportunity, and Work with Accelerated Mobility, Efficiency, and Rebuilding of Infrastructure and Communities throughout America Act.

mostly in transportation. The proposal includes a number of potentially controversial elements, including new funding for high-speed rail and public transit; there is also pressure for a political compromise, as funding for the Highway Trust Fund is about to run out.[16] Historically low interest rates and persistently high unemployment numbers create strong incentives to push ahead with infrastructure spending now, despite strong popular opposition to higher taxes and government spending more generally. The big question will of course be whether the proposed infrastructure development plans will be derailed by partisan gridlock, tensions with subfederal governments, or efforts to hijack federal funds for pork barrel projects.

Cybersecurity as a political lever?

Second, the current apprehensions about cybersecurity, particularly in the United States, could be a source of political momentum for the broader CISR agenda. One of the most obvious patterns in the last twenty years is that high-profile crises can be counted on to attract a burst of political attention to the relevant issue or sector, which can in turn lead to significant progress in making and coordinating national policies. The 2003 Northeast Blackout, for example, focused attention on the electric grid in the mid-2000s, and the resulting push to show concrete results is an important reason why CISR cooperation in this area is more advanced and more institutionalized than in other, comparable parts of the energy infrastructure agenda.[17] The new focal point for attention to CISR, of course, is cybersecurity, based on controversy over cyber incursions by hackers based in China and Russia.[18] Cybersecurity has become an obsession in Washington over the last few years, and a number of government agencies and industry associations have recently issued public warnings that various critical infrastructure sectors are vulnerable to disruption by cyber attacks. Virtually all kinds of critical infrastructure today have both a physical and a cyber architecture, and it makes little sense to try to secure one of the two layers in isolation from the other. The nature

Virtually all kinds of critical infrastructure today have both a physical and a cyber architecture, and it makes little sense to try to secure one of the two layers in insolation from the other.

[16] Damian Paletta, "US to Reduce and Delay Highway Funding Beginning in August," *Wall Street Journal*, July 1, 2014. [http://online.wsj.com/articles/cuts-in-highway-funding-to-start-in-august-1404231868?mod=rss_US_News]

[17] The industry-led regulatory body which governs electricity generation in the United States and Canada—the North American Electric Reliability Corporation (NERC)—goes well beyond just publicizing best practices, having been empowered to impose financial penalties on individual providers that fail to live up to industry standards. [http://www.nerc.com/Pages/default.aspx]

[18] Widespread concern about cybersecurity in Washington was first triggered by the so-called "botnet" attacks on US government websites in July 2009.

of the cyber challenge is evolving rapidly, the contours of the policy debate are as yet unformed, and there is a clear opportunity to frame the issue in ways that would renew political attention to both physical and cyber aspects of critical infrastructure.

Two priorities have emerged in recent US debates on cybersecurity, each of which is being followed up with new legislative proposals. One priority is the creation of a framework for closer public-private collaboration, with special attention to the creation of voluntary business standards and practices. Executive Order 13636 directed the National Institute of Standards and Technology (NIST) to work with the private sector to develop a general framework, which was unveiled in February 2014. A handful of bills are in play to further this priority, including S. 1353, which calls for clear rules governing the protection of private and proprietary information, and would provide additional resources for research and information-sharing.[19] A second priority is the clear designation of a lead agency to coordinate cybersecurity efforts, and to establish sector-specific councils for inter-agency and public-private consultation leading to sector guidelines and plans, as in the broader CISR effort. One of the more prominent possibilities here is H.R. 3696, which clearly establishes DHS as the lead agency.[20] If passed, H.R. 3696 would reinforce the conceptual and bureaucratic links between cyber and physical infrastructures, expand the pool of resources that could be applied to CISR broadly-conceived, and allow for differentiated approaches across the various sectoral contexts.

Increased concern about cybersecurity has already prompted some new diplomatic engagement, though so far this is limited to the US-Canada bilateral relationship and is apparently oriented to following national policy choices, rather than influencing them. The October 2012 Cybersecurity Action Plan pledges DHS and PS to consult more closely with one another about national emergency-response planning, strategies for engaging with the private sector, and public awareness campaigns.[21] The plan in its current form is clearly inadequate, but represents a useful starting place for more ambitious forms of bilateral or trilateral coordination, which could more effectively link up cyber and physical infrastructure agendas.

Recommendations

Restarting the conversation, rethinking the problem

The challenge for CISR advocates now is to develop long-term strategic plans that go beyond information-sharing and best practices, and ultimately develop incentives to encourage public-

[19] Reported to committee in February 2014.

[20] Reported to committee in February 2014.

[21] Cybersecurity Action Plan between the Department of Homeland Security and Public Safety Canada. [http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cybrscrt-ctn-plan/cybrscrt-ctn-plan-eng.pdf]

and private-sector managers to make real investments in CISR. Current efforts are mostly focused on the development of sector-specific plans, which are mainly concerned with overcoming technical obstacles to closer CISR cooperation, such as the development of information-sharing platforms that can credibly reassure private sector stakeholders about the confidential handling of sensitive or proprietary information. There is nothing surprising or problematic about the fact that the CISR agenda has shifted from very general discussion of concepts and priorities to much more fine-grained, sector-specific consultation about the day-to-day practice of information-sharing and scenario planning. Those sector-specific, technical consultations should of course carry on, and indeed should be accelerated where possible. But it would be a mistake to put all of our energies into sector-specific initiatives, or—even worse—to assume that since we have "moved on" to sector-specific initiatives, the broader, strategic agenda has been resolved. There needs to be a continuation of—and indeed a renewal of—bird's-eye-view strategic planning on CISR to shift the agenda from "making plans to make plans" to the creation of robust national and regional strategies. These strategies must prioritize CISR efforts and move from political spending "commitments" to concrete expenditures on public-sector infrastructure projects, and—perhaps most difficult of all—develop a set of incentives and constraints to effectively influence private sector decision-making.

DHS, Public Safety Canada, and CISEN should therefore create a trilateral expert panel to develop a strategic framework for long-term CISR planning in North America, mapping out a set of goals, timetables, and spending commitments.

DHS, Public Safety Canada, and CISEN should therefore create a trilateral expert panel to develop a strategic framework for long-term CISR planning in North America, mapping out a set of goals, timetables, and spending commitments. This panel would be more proactive and strategic in its approach than the existing cross-sector forums developed to provide a "bigger-picture" view of progress under the US NIPP, which in practice have mainly been concerned with preventing frictions across existing sectoral efforts. This new expert panel would be charged with working out a three-year strategy to get past the current impasse, with particular attention to "re-booting" the working relationship between public- and private-sector players.

CISR as corporate social responsibility

Movement toward the next phase of CISR cooperation need not involve extensive new government regulation, though of course some new regulations may be appropriate, particularly in sectors where industry is fragmented and has little experience with effective self-

regulation.[22] Targeted tax incentives may also be appropriate in some cases, particularly where research clearly demonstrates that the tax revenues foregone in this area would in the long run be less than the costs associated with having to rebuild after a major critical infrastructure failure. In terms of policy instruments, the focus should in most cases continue to be on providing information about CISR risks and benefits, and, in the longer term, on cultivating a deep-rooted commitment to CISR principles among critical infrastructure operators in both the public and private sectors.

In the mid-2000s, significant effort was made to raise awareness and provide technical background to key audiences such as legislators, subfederal government officials, the media, and academics, but that effort has tailed off over the last few years. As part of a broader campaign to push CISR cooperation to the next level, these public outreach efforts should be renewed, through the initiation of a series of expert presentations designed to play up the connections between CISR and other current policy choices (e.g., counterterrorism, stimulus spending, cybersecurity).

Many industries have been successful in developing their own "self-regulating" professional standards and practices through their absorption of a set of shared principles for corporate social responsibility (CSR). Given that most of the critical infrastructure in North America is privately owned and operated, and that there is little appetite for imposing costly new regulations on these private operators, national security planners and industry associations in all three countries should be actively trying to promote CISR as a key CSR norm for North American business.[23]

Renewing regional dialogue

Given that most of the obstacles to CISR cooperation are domestic and political, an argument could be made for giving up on regional coordination—at least for now—until the necessary domestic political changes have been made, or at least until the domestic political climate is more favorable. But regional consultation is still crucial to

Regional consultation is still crucial to the success of national CISR efforts.

[22] The most ambitious of recent regulatory efforts within the US CISR agenda has not been much of a role model for other sectors. DHS's Chemical Facility Anti-Terrorism Standards (CFATS) program has struggled with the clarity of its guidelines, the timeliness of its review process, and the overall level of compliance from industry participants.

[23] The general argument for framing compliance with CISR standards as corporate social responsibility is developed in Gail Ridley, "National Security as a Corporate Social Responsibility: Critical Infrastructure Resilience," *Journal of Business Ethics* 103 (2011): 111-125.

the success of national CISR efforts. The obvious and important reason for this is the interdependence of national systems, particularly in sectors such as electricity, banking and finance, and telecommunications. If CISR efforts are not properly aligned among North American partners, disruptions may not be effectively contained, emergency responses may be slowed or rendered ineffective, and uncertainty about policy compatibility may undermine confidence in infrastructure services. The less obvious reason is that diplomatic commitments made as part of regional (or bilateral) policy coordination initiatives can have important effects on national policy development, sustaining momentum for a coherent national strategy against legislative, bureaucratic, or local political spoilers.

The long, slow process of network-building around CISR issues that began after 9/11 is kind of like rolling a big rock up a hill: it takes a lot of work to keep things moving, but it would only take a small lapse of effort to lose all momentum and send the process back to the beginning. The difficulties already encountered just in getting people together to talk about these issues and to agree on basic concepts and standards, help us appreciate the technical and political difficulties that will undoubtedly be encountered in the next phase of the process. CISR cooperation will move on to prioritize some sectors over others, develop concrete plans, pool resources for emergency response, and make the costly investments that will be required to build up meaningful security and resilience. The fact that this will be difficult, however, should not distract us from the fact that it is necessary.

About the Author

Brian Bow is the Director of the Centre for Foreign Policy Studies and an Associate Professor at Dalhousie University. He is currently a Senior Fellow at American University's Center for North American Studies and a Fellow at the Canadian Defence and Foreign Affairs Institute. He has previously been a visiting researcher at the Woodrow Wilson International Center for Scholars, American University, Georgetown University, Carleton University, and the Australian National University. Dr. Bow holds a Ph.D. from Cornell University, a M.A. from York University, and a B.A. from the University of British Columbia. Most of his current research is on North American regional politics, U.S.-Canada, and U.S.-Mexico relations.