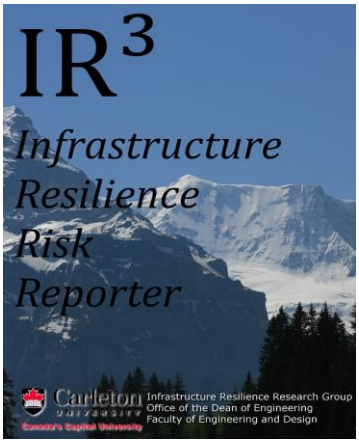
VOL 1 ISSUE 1

April 2014



IR3 Feature Articles

Editorial Corner

Angela Gendron

The Infrastructure Risk Resilience Reporter (IR3) has been launched to facilitate information-sharing amongst stakeholders in Canada's infrastructure from both private and public sectors – executives, practitioners, academics, students. The editors propose to publish articles in due course which review leading edge, interdisciplinary contributions to the professional literature. In our inaugural issue, we have asked practitioners in the public and private sectors to share with readers their experience and assessment of practical information-sharing initiatives. We welcome comments from readers pertaining to any article published in the IR3; suggestions on content for future issues; proposals for articles (generally within a 5000 word limit); and information about any books or reports relating to the resilience of critical infrastructure (CI) that is likely to be of professional interest to others. We have in mind soliciting book reviews in due course. References to books, abstracts of articles and literature/book reviews will be found in the 'Literature Corner' at the end.

The focus in this inaugural issue is on ***information-sharing***. We begin with an editorial perspective on resilience and the new security environment, followed by two articles on information-sharing based on the experience of contributors, Nicole, Head of Critical Infrastructure, RCMP and Doug Powell, Manager, Security, Privacy and Safety, BC Hydro. Nicole discusses the Significant Incident Reporting System (SIRS) and its role in the rail terrorism arrests last year. Doug reviews the information-sharing arrangements with which he was involved during the 2010 Vancouver Games.

In addition, since information-sharing can be a subject which generates some heat, a review of the research work of Jacques Shore on the legal and moral obligation to share is also included. Under Canadian federal law, any disclosure by the private sector of security, data breaches, detected incidents or intrusions are strictly voluntary, as is compliance with public regulatory standard CAN/CSA Z731-03, but there are legal implications for government and private sector owners and operators who are not compliant. Jacques Shore has expressed his view that something more is needed.

Resilience and the New Security Environment

Angela Gendron

Canada faces significant challenges in preparing for, withstanding and recovering from disasters whether caused by natural hazards, such as severe weather and flooding or by accidents or deliberate human activities. The disruption or destruction of national critical infrastructure assets and services threatens the ability of regions, cities and enterprises to function effectively and puts at risk the safety and economic and social well-being of citizens.

Reference to the 'new security environment,' is now commonly used to describe not only a greater diversity of threats and hazards than hitherto, but a changing perception of what we mean, or should mean, by 'security' and the security architecture needed to adequately protect our society from 21st century threats and risks. Seemingly unrelated events have cumulatively signalled the need for a highly co-ordinated response which differs qualitatively from what has gone before. Technological developments over the past twenty years have provided social and economic opportunities, but they have also introduced new and growing vulnerabilities. The challenge is to ensure that our security architecture is adaptive and adequate for its purpose.

The fragility of our modern economic and social infrastructure and its susceptibility to disruptions, derives from global markets, just-in-time supply chains, complex interdependencies within and between critical infrastructure sectors and the ubiquity of cyber connections which make all sectors highly vulnerable. As a consequence, responsible authorities have accepted the need to revisit former perceptions of 'normality' and consider whether and how resilience needs to be enhanced.

Risks, Threats and Resilience

Deep uncertainties arise when the probabilities of outcomes are poorly known, unknown, or unknowable. In such situations, past events may give little insight into the future, yet predicting the probability of an event is of paramount importance to mitigation strategies. A recent survey[1] of the vast literature on risk concludes that the most useful definition of risk is derived from answers to the following questions:

1. What can happen or what can go wrong?
2. How likely is it that it will happen?
3. If it does happen, what are the consequences?

Traditionally, the harms from which we needed protection were perceived as those posed to national security by hostile states, their armies and agents of espionage, but modern networked and interdependent societies are now inherently more vulnerable. While protection is still needed from these and a growing pool of non-state actors (such as terrorists operating from both outside and inside our borders), the diversity of threats and the reality that hostile actors need only be 'lucky' once, means that intentional threats must now be considered within a broader national resilience framework of measures to withstand, mitigate and recover from the impact of a successful attack.

Indeed the concept of national security has been changing in recent years so that it is now perceived as covering the responsibility of government to tackle a range of threats to individual citizens, families and businesses. The need to manage these risks so that 'people can go about their daily lives freely and with confidence in a more secure, stable, just and

[1] Peter Gill, (2012) 'Intelligence, Threat, Risk and the Challenge of Oversight' *Intelligence and National Security*, 27:2, 206-222 p207

prosperous world' has become a broad security aim in the UK and elsewhere.[2] The resource implications of this more 'human' view of national security are tempered by the principle of subsidiarity - authority and information are pushed down so that local problems can be tackled at a local level.

Subsidiarity is also a governing principle of Canada's approach to managing risks. It has adopted an 'all-hazards' or all-inclusive approach to potential harms because it considers changing weather patterns, natural disasters, outbreaks of human and animal disease, industrial action and civil unrest to be as damaging as terrorism. Indeed, on an index of relative impact, pandemic flu, coastal flooding and major industrial accidents rank higher than terrorist attacks.

Threat and risk assessments both attempt to calculate probabilities multiplied by harm. The difference between them is that threats are defined as explicit intentions to cause harm while risks are events that might cause unintentional harm. Traditionally, protective security measures were applied to 'unknowable' malicious threats based on assessments made by intelligence agencies while resilience measures protected against the more 'knowable' or quantifiable harms associated with natural hazards and safety risks, such as those assessed by businesses and health agencies.

Reliable actuarial calculations can be made about the potential harms of frequently occurring incidents with predictable outcomes. This is not possible for low probability events for which the potential consequences are unknown or incalculable – though there are models attempting this. In the new security environment, the growing uncertainties associated with weather volatility are making it more difficult to develop appropriate levels of mitigation.[3]

The Conflation of Threats and Risks

A more inclusive security regime which recognizes these growing uncertainties and the overlap between threats and risks, looks towards resilience policies to provide protection for a range of different hazards along a continuum of threats and risks. Protective security measures alone cannot guarantee the continuity of infrastructure operations against threats. Furthermore, the perceived increase in the uncertainty of risks, as well as, threats and the consequent pressure to act in a *precautionary* manner, has brought intelligence work into greater proximity with areas of risk, such as finance and law enforcement. Intelligence-led policing, for example, can help prevent and reduce crime rates just as resilience measures can mitigate the effects of an opportunist espionage or terrorist attack which succeeds despite protective security measures. Both must be supported by resilience strategies which build the capacity to withstand or rapidly recover from disruptions or destruction.

[2] The National Security Strategy of the United Kingdom, Cabinet Office 2008 p5].

[3] The economic impact of increasing everyday weather volatility in Europe exceeds the huge sums that are annually associated with natural catastrophes.

Bringing safety risks into a more inclusive and joined-up security architecture has many potential advantages including the more efficient allocation of resources. The importance of adequate flood defences, for example, might be valued on a par with preventing violent extremism. However, authorities need methods by which to determine how they can use their limited resources in the best possible way in the face of uncertainty.[4] Selecting an optimum mitigation strategy depends on estimating the expected value of damage which in turn requires an ability to predict the probability of disasters.

Cross-Canada Consistency

Achieving cross-national consistency in security and resilience practices, expenditures and standards will be a challenge in Canada's multi-jurisdictional confederation of provinces and territories. In this respect, Public Safety Canada (PSC) has a crucial role to play in providing the necessary central leadership for a more holistic, inclusive security architecture the success of which will depend upon the promotion of closer relationships between multiple private and public sector partners and contributors. Resilience planning, information-sharing, multi-agency training and exercising will be essential elements alongside according greater recognition to the role and importance of front-line responders and emergency services.

Security is delivered not just by law enforcement and intelligence agencies, such as CSIS, but emergency planners in central, provincial and municipal government, Fire and Rescue Services, Health Canada, Environment Canada, Natural Resources Canada and many other public and private sector agencies and enterprises. Further, these various agencies and emergency responders also work with the military, NATO and the voluntary sector in their peacekeeping roles and in the provision of humanitarian aid. Joining up these efforts within Canada and in operations overseas is a prerequisite for ensuring security in a changing environment.

In conclusion, while the distinction between old and new definitions of security is relatively clear, achieving an inclusive appreciation of security against all-hazards is more elusive. A strong national resilience framework is needed to push forward measures to tackle the diversity of threats and risks to national infrastructure since there are many hurdles to overcome. Information-sharing is certainly one of them. The greater involvement of emergency responders and other partners means that levels of security clearance differ and this militates against sharing. Perceived risks to sensitive data, companies' concerns with reputational issues, information privacy and due diligence are further impediments. Yet

---

[4] Jerome L. Stein and Seth Stein, "Formulating Natural Hazard Policies under Uncertainty," *SIAM/ASA Journal on Uncertainty Quantification* 1, no. 1 (27 March 2013): 42–56)

information-sharing is essential if knowledge is to be gained about infrastructure interdependencies, consequences and risk.[5]

The diversity of threats we face in the 21st Century, as defined by a modern understanding of 'security,' means that in practical terms we have little choice but to engage more actively with others in sharing–information, which may have a bearing on their safety and well-being. There is certainly a moral, if not legal, obligation to do so.

---

[5] Acknowledged as one of the seven core tenets of the US National Infrastructure Protection Plan, 2013 (NIPP).

RCMP Critical Infrastructure Intelligence Team: An Overview

Nicole Murphy, Critical Infrastructure Intelligence Team, Federal Policing Criminal Operations, Royal Canadian Mounted Police

Threats to critical infrastructure can come in many forms; including from biological, chemical, radiological, nuclear, explosive devices, and from computer viruses. Criminal threats to Canada's critical infrastructure include those which prevent, interfere with or delay the production or delivery of the essential services that are required to ensure the health, safety, security and overall well-being of Canadians. These threats extend beyond terrorism to include crimes ranging from property crime, serious and organized criminal activity, foreign state interference, criminal extremism, anarchism and cyber threats.

Canada is not immune to the threat from terrorism. This was demonstrated by law enforcements' disruption of two terrorist plots in 2013; one targeting rail infrastructure, and the other a provincial government building.

On 2013-04-22, the RCMP arrested two men and charged them with conspiring to allegedly carry out a terrorist attack against CN and VIA assets. The accused, who are both in custody, are charged with conspiring to carry out an attack against, and conspiring to murder persons unknown for the benefit of, at the direction of, or in association with a terrorist group.

On 2013-07-01, the RCMP arrested two individuals alleged to have targeted Canada Day celebrations at the Victoria Legislature in British Columbia. The pair were allegedly intending to use multiple pressure cooker bombs that appeared similar in composition to the recipes outlined in *Inspire* magazine. They have been charged and are in custody.

Most terrorist attacks are preceded by pre-attack indicators that can be identified, reported, analyzed and acted upon. Suspicious incidents, such as phone calls from potential customers asking unusual questions about security or business processes, or individuals taking photographs of a facility in a manner unusual for tourists, may not typically, garner the attention of law enforcement, however, these suspicious incidents might be an indicator of terrorist pre-incident planning or other serious organized criminal activity. The reporting of these indicators, when put in a broader context, could help prevent an attack.

Critical Infrastructure Intelligence Team (CIIT)

As Canada's national police force, the Royal Canadian Mounted Police (RCMP) plays an important role in the protection of Canada's critical infrastructure, has the primary responsibility to prevent, disrupt and investigate terrorism-related criminal activities in Canada. The Critical Infrastructure Intelligence Team (CIIT) examines criminal threats to critical infrastructure in support of the RCMP's and Government of Canada's critical infrastructure protection mandates and to support RCMP investigations of these threats.

CIIT collaborates closely with domestic partners at the federal and provincial government levels, as well as, other law enforcement groups and private sector stakeholders to protect critical infrastructure. CIIT directly impacts investigations through its interaction with the private sector and other government and police partners to ensure support to, and initiation of, RCMP investigations both domestically and internationally.

CIIT's current focus is on collecting and analyzing intelligence on criminal threats to Canadian critical infrastructure in six of the 10 critical infrastructure sectors defined by Public Safety Canada – Energy and Utilities, Finance, Transportation, Government, Information & Communication Technology, and Manufacturing.

Suspicious Incident Reporting (SIR) System

CIIT developed the Suspicious Incident Reporting (SIR) system – a secure web-based portal – to gather information from industry, government and law enforcement about suspicious incidents that may indicate a potential criminal threat to Canada's critical infrastructure.

There are currently SIR users from the public and private sector representing Energy and Utilities, Finance, Manufacturing, Government, Information and Communication Technology, and Transportation sectors.

SIR is a cornerstone of the RCMP's critical infrastructure protection initiatives, directly supporting the RCMP's mandate to detect, deter, disrupt, and investigate threats to Canadian critical infrastructure. The system has shown itself to be valuable to both the RCMP and to private sector stakeholders, with tangible progress made towards sharing information and intelligence on indicators common to criminal activity relating to critical infrastructure.

SIR is designed to collect information from CI stakeholders on where, when, and how suspicious incidents in Canada are unfolding overtime. The system allows CI stakeholders to submit information on suspicious incidents affecting their security and operations directly to the RCMP. This information is analyzed against information and intelligence from other sources to develop intelligence products for the benefit of the law enforcement and intelligence community, as well CI owners and operators. The production and dissemination of intelligence products provides the base for an effective and healthy information exchange which will, ultimately, enhance the protection of Canada's CI. These products also become part of a secure online library that can be accessed by security-cleared CI stakeholders.

SIRs submitted by CI stakeholders are leveraged by CIIT to support both criminal and national security investigations and provide the RCMP with key early-warning intelligence to assist external stakeholders with CI resiliency. In terms of potential threats to critical infrastructure, the most notable, in 2013, included criminal activity inspired by foreign and domestic criminal extremism inspired by specific ideological causes. The majority of SIRs in 2013 involved incidents of sabotage, tampering or vandalism to CI assets, an expressed or implied threat to a facility or employee, and suspicious photography.

Suspicious Incident Reports in 2013

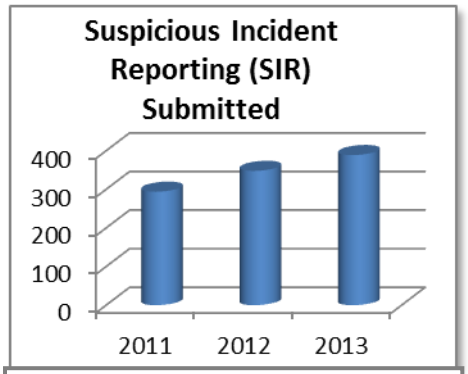
- In the month of May 2013, CIIT received SIR reports from stakeholders within the energy and chemical sectors regarding suspicious activity around their facilities. All reports were generated from a specific geographical location in southwestern Ontario. Activities included taking photos and videos of CI, trespassing, and one incident of mischief to property. Vehicle licence plates and descriptions of numerous persons of interest have been provided by stakeholders to law enforcement. This identification of such incident clusters as this one demonstrates how reporting from a variety of stakeholders allows law enforcement agencies to identify individuals who may pose a threat to CI.

- In 2013, CIIT received SIR reports from stakeholders within the finance sector. Half of these reports were evenly distributed among the categories of fraud, vandalism, suspicious person on premises, and threatening correspondence. The remainder of these reports involved individuals engaging in activity commonly associated with the Freeman on the Land (FOTL) and other similar movements. These movements have been characterized as having a decentralized, libertarian ideology with a substantial on-line presence. The SIR reports commonly associated with these movements primarily involve a pseudo-legal document referred to as a "Claim of Right". This document includes language that conveys a nonsensical interpretation of the law, and the writer's unwillingness to consent to it. Followers of these movements use these documents to declare their sovereignty, and as a means of trying to gain access to fictitious funds from financial sector executives and/or government officials.

A Shared Approach

The interconnected nature of Canada's critical infrastructure makes partnerships among law enforcement, government, and critical infrastructure owners and operators vital to manage risks, reduce vulnerabilities and strengthen the resiliency of critical infrastructure across all sectors. The RCMP recognizes the importance of sharing intelligence with CI owners and operators to ensure they have access to accurate criminal intelligence of potential and credible criminal threats against their assets, as they are ultimately responsible for ensuring the resiliency of Canada's critical infrastructure.

A significant proportion of Canada's critical infrastructure is managed and protected by private owners and operators. These CI owners and operators have established emergency responses and business continuity plans to ensure the uninterrupted supply of vital services, however, it is not possible for owners and operators to be aware of all potential criminal threats. Perhaps most importantly, private industry is in the best position to observe what is, and is not, normal behaviour at and around their facilities and to report the suspicious incidents or behaviour to law enforcement. Also, CI owners and operators possess information about the potential vulnerabilities of their assets and the risks involved if targeted. In short, to produce intelligence assessments to support the private sector in the protection of their assets, CIIT needs an exchange of information with industry to ensure the intelligence, and assessments, provided are relevant, accurate, timely and actionable.



Source: RCMP SIR Database

CIIT's private sector stakeholders recognize the benefits of collaborating with the RCMP to assist in the protection of their operations. This is demonstrated by the steadily increasing number of suspicious incidents that are reported through SIR and the corporate information industry is willing to entrust to CIIT, information that has been directly responsible for the early detection of potential criminal activity and which has contributed to RCMP investigations.

Beyond the normal parameters set out for information-sharing, when the RCMP becomes aware of potential threats to CI, partners are advised early-on in the process of sensitive criminal investigations. In 2013 there were incidents involving threats targeting CI assets

and facilities where the RCMP advised CI security partners directly on matters that were of potential concern to the continuity of their operations.

Over the last several years CIIT has developed mutually respectful partnerships with public and private CI stakeholders and other law enforcement and intelligence partners. An example of these crucial partnerships is CIIT's long-standing relationships with CN Police and VIA Rail. These partnerships proved extremely useful over the course of the investigation. For several years, CIIT has enjoyed a close relationship with both of these organizations and when approached, CIIT's contacts did not hesitate to provide their assistance at every turn. These partnerships meant CIIT had a direct line into specific information on rail infrastructure, which assisted law enforcement in gaining a more complete picture of potential threats and confirmed there was no imminent threat to the general public, rail employees, train passengers or infrastructure. The investigation demonstrated the value of close relationships between law enforcement and owners and operators of critical infrastructure.

For the RCMP to be successful in its efforts, it cannot be done alone. Protecting Canada's national security requires the awareness and the engagement of everyone. CIIT continues to develop and maintain crucial stakeholder operational contacts across CI sectors to support the exchange of intelligence and information that supports owners and operators in protecting their critical assets, while supporting RCMP investigations.

CIIT encourages its partners to report information regarding suspicious or criminal activity to local law enforcement.

To report information regarding suspicious activity, criminal extremism, or other activities which could pose a threat to Canada's national security, call:

National Security Information Network (NSIN) at 1-800-420-5805
Canadian Security Intelligence Service (CSIS) at (613) 993-9620

For more information on the RCMP's SIR system, please contact: SIR-SIS@rcmp.grc.gc.ca

---

The 2010 Winter Olympics Model

Doug Powell, CPP, PSP

As head of security for BC Hydro since 2006, Doug provided guidance to protect critical infrastructure during the 2010 Winter Olympic games in Vancouver. He now manages Security, Privacy and Safety risk for smart metering at BC Hydro. Doug has 30 plus years' experience managing security and is an expert in several areas related to critical infrastructure protection and security planning. He serves on several International committees and professional organization; is an advisor to Canada's National Electricity Infrastructure Test Centre (NEITC) and participates as a research and education Associate for the Infrastructure Resiliency Research Group, Carleton University.

Introduction

Information-sharing between industry partners is typically done in a closed, pens-down environment with discretion applied. Information-sharing between industry and police, industry and government or industry and intelligence agencies has always been challenging for many reasons. Prior to the start of the 2010 Olympic Games, information-sharing was centre stage as the provincial emergency management program sought to engage industry on emergency response planning. This required an understanding about key infrastructure within the Olympic theatre of operations and a study of interdependencies between various infrastructure owners. Without this level of rigour, it would have been impossible to identify critical infrastructure and critical infrastructure dependencies related to the Olympic Games. But getting to this point was a complex task even though the emergency management community within Greater Vancouver and across British Columbia already enjoyed a mature level of collaboration and dialogue.

The Partners

Key players in the 2010 Winter Olympic Games information-sharing initiative were: police from numerous jurisdictions, as well as, police support agencies; Canadian military; Emergency Management BC; industries representing the ten Canadian sector networks and foreign government agencies and industry representatives from the USA. Only those organizations identified as primary contributors and infrastructure asset owner/operators were invited to confidential information-sharing sessions. The Integrated Security Unit (ISU), an RCMP led security group made up of many different policing groups, was the designated lead in the information-sharing initiative. Emergency Management BC had the lead in information gathering practices.

The ISU for the 2010 Games was, in itself a complex group made up of many different agencies who needed to establish communication protocols, hierarchical relationships and confidentiality (need-to-know) restrictions. Public Safety Canada which took the lead in national security and emergency management/emergency preparedness initiatives, was also operating under increased scrutiny following a 2009 report by the Auditor General of

Canada which made specific recommendations for improving Canada's posture in the area of Emergency Management. All combined, there was a peaked interest in seeing Canada's emergency program advanced and fine-tuned in light of the pending Olympic Games. New reporting and organizational structures were being planned and introduced as the Olympic Games preparations proceeded. With policing and intelligence playing a key role in the security plan for the Olympic Games, the structure used for gathering and coordinating information was an emergency management framework. Defaulting to a general belief that critical infrastructure owners/operators were capable of meeting protection standards for their assets, the focus for the ISU was to identify response issues in the event of a critical event.

Objectives

The primary objective for information-sharing for the 2010 Games was to protect infrastructure so as to provide a safe operating environment for the Games. It was also to ensure that those living outside the Olympic operating theatre would not be adversely affected by any security incidents. Best efforts were made to identify critical infrastructure within the theatre of operations, to determine infrastructure interdependencies and apply appropriate protection and support to this infrastructure for the duration of the Games.

The focus was on emergency response using prevention as a key driver to minimize the potential for adverse impacts on infrastructure. This created governance challenges both in relation to collecting information from infrastructure owners and operators, as well as, in sharing information and intelligence with local infrastructure owners who prioritized protection of assets over response to adverse incidents. While the ISU did its best to present a comprehensive and coordinated process for the collection and control of information, there was some misalignment related to process. Furthermore, this initiative was new and untested in Canada and had some important hurdles to overcome. These included mutual trust levels between industry, government and police as well as confidentiality agreements which related to collection, use, collation and deletion of the information being collected to satisfy infrastructure owners that their information was well-managed and protected. The way in which this was overcome not only led to new understandings, new programs and new relationships between industry and government, but created a new understanding and new playing field for information-sharing amongst all critical infrastructure players in Canada. While this process is still not perfect four years after the 2010 Winter Olympic Games, great leaps forward have been achieved in terms of building trusted relationships which far exceed similar programs in other countries.

The Information Gap

Prior to the coordinated planning effort for the Olympic Games in Vancouver, Natural Resources Canada (NRCan) had already initiated a model for sharing some classified information generated by police and intelligence agencies. Approved industry representatives from the energy and utilities sector in Canada, are cleared to "Secret" level under the same provisions as government employees and invited to attend classified briefings.

Within this secure environment, sensitive information can be shared by government agencies with industry partners who in turn can discuss sensitive company and industry issues relating to critical infrastructure. This enables both sides to have a meaningful dialogue on national and regional security issues and develop trusted relationships. The collaboration between police, intelligence agencies and industry partners extends to the sharing of risk information, threat trends, adversary capabilities and protection profiles. It has led to the development of other intelligence products like threat assessments and incident reporting on a national scale.

During preparations for the 2010 Olympic Games, however, many more players were involved who were not security cleared, but wanted classified and sensitive information for purposes other than communicating threats and facilitating protection. Still, developing an effective emergency response capability on a regional basis was very important to the success of the Games and some information about critical infrastructure assets across numerous sectors was central to a program for prioritizing responses.

Framing the Problem

The problem in divulging information from industry's perspective was the potential to have information about its most sensitive asset and operational plans in the hands of government agencies whose best interests were to share and cross-reference this information which potentially could be released into the public domain. Loss of control over information concerning critical infrastructure vulnerabilities and asset placement, especially when collated and stored in one place, would be a gold mine to any protest or extremist group. In an environment like the Olympic Games where global social issues are often played out for the media with the Games as a backdrop, the release of sensitive data seemed contrary to effective protection. This posture put the interests of industry in direct opposition to the interests of the emergency management and policing groups who were seeking information.

The central issue in this was trust. There was an apparent lack of trust that government agencies in any form were capable of effectively managing industry's deepest security secrets. The focus of this mistrust related to government ability to protect and control information given to them. This included cyber-security on government servers, data protection on agency servers, the inadvertent or purposeful sharing of industry information with other government groups and international partners within the Olympics integrated security domain, as well as the long term implications of having industry data in the hands

of police and emergency management personnel. There was a concern that diligence around data protection could become more casual or careless over time. Once information is lost, control cannot be regained.

While critical infrastructure owners were working diligently to remove sensitive data from the public domain, it became apparent that an abundance of open source information about industry partner assets was already available through internet searches and other means. Industry assets already existed on government generated materials from years past. It is true however that insider knowledge about these assets was necessary in order to confirm the criticality of any such asset. Also, without detailed information about particular assets, it would have been very difficult to determine the dependencies of particular infrastructure. Applying protection to specific critical infrastructure was necessary to prevent the possibility of a more profound impact across multiple infrastructures. For example, transportation of emergency personnel could become impossible if one particular bridge was removed and if the bridge was also carrying a main communications cable over the water, it would have an impact on regional telephone systems. Once these asset nexus points were better understood, they were prioritized in terms of their importance for protection. Seeking industry's input was therefore vital.

The Solution

Ultimately, through considerable dialogue, there was agreement to share this information about critical information and assets. A three-tiered sharing model was designed and implemented allowing industry stakeholders a choice as to how much information they wished to share about their assets. The three available options included: limited sharing in a protected manner (no assets named, but critical functionality of assets and their relative placement provided); a moderate disclosure under which assets could be named and location provided, but more sensitive vulnerabilities and criticality issues left off the record; or full disclosure in which the entire record of the company was delivered and nothing held back. In the first case, where assets were identified but not named, they were given a criticality ranking. An emergency protocol existed which required that, following a major emergency event, the industry partner would be consulted to provide more information about the asset so that coordinated decision-making would be possible. In the case of "moderate sharing", a similar situation existed, but the coordinating body was able to plot assets and name them in their integrated map. With full disclosure the coordinating body was able to plot and hold full asset information.

Before industry partners submitted their survey forms, a non-disclosure agreement (NDA) between the RCMP (lead organization of the ISU) and the industry entity was prepared and signed. Within the context of the NDA, the industry partner had the right to request deletion of all of their data, as supplied in the information transfer, once the Games had concluded. This was done in a prioritized fashion. The first group required to delete and destroy all such data was the ISU, as well as any other agency that had permission to view this data within the context of Olympic Games protection and response. The RCMP itself was then permitted to retain the data for approximately one year longer before it too was required to delete it. Ultimately, the industry information provided for Olympic Games

emergency management and protection planning could not be retained by any government body or agency beyond the use of Olympic Games management unless there was specific permission given by the industry partner who submitted it. This included the retention of industry data in new formats that were a derivative of the industry supplied data.

In 2009 acceptable NDAs were signed and industry partners began evaluating their infrastructure using an asset rating system supplied by Emergency Management BC to identify criticality rankings. That survey information was submitted to the RCMP for protected use. Accountability for all information supplied rested with the RCMP as lead in the ISU. This information was not provided to any other agency without the permission of the industry entity who supplied it. A well-defined governance model was implemented to ensure full trust and full accountability. In addition, security clearances initiated by the ISU began to address individual personal reliability assessments and provided assurances that those participating in group information sessions met a reasonable expectation of trust. Nevertheless, note-taking and document distribution was at a bare minimum during meetings. Mandatory participant introductions at each subsequent meeting ensured full disclosure about who was in the room.

Through this information-sharing model, some excellent collaborative work resulted. Asset mapping and nexus plotting not only served to inform the integrated services about critical infrastructure, but for the first time in British Columbia, asset owners began to understand and plot their own dependencies and protection requirements. This is not true of all critical infrastructure owners, but was certainly true of many if not most. In retrospect, this Olympic exercise moved emergency management and critical infrastructure protection years ahead in this region. It served as an excellent model for information-sharing and collaboration and brought trust to a new level. Were it sustained, and many efforts have been made to emulate this model across the country, Canada would stand out as a world class example for emergency planning and national security.

Additional Spin-offs

The model described in the previous section was comprehensive and very important to pre-Olympic planning efforts as discussed. But other information-sharing practices seemed to spring forward following this process which demonstrated not only refined and intentional collaboration, but also served as an example as to what is possible in the right operating environment. As the months passed, and as the ISU took shape and key personnel were identified, industry partners, especially those controlling the most critical infrastructure in the Olympic theatre, began to share information in one-to-one meetings and through work process. This included providing police resources, insight into protected industry assets, the sharing of engineering documents, and looking at specific industry protection plans.

This type of sharing, not previously requested of industry, was unprecedented. It gave police agencies direct access to and knowledge about critical infrastructure so that Olympic protection planning could be carried out strategically and with the most efficient deployment of resources. Understanding where critical assets exist helped the Olympic Games security planners identify where more protection needed to be assigned. This was

applied in the form of mechanical and technological protection mechanisms, as well as the assignment of personnel and security processes like targeted patrols of underground infrastructure on a daily basis.

In return, industry requested information from police and intelligence agencies that allowed the industry entity to plan protection based on accurate threat information and to integrate police response and intelligence resources for critical problems arising throughout the Olympic Games period. With prior knowledge, industry was able to direct policing resources to hot spots and suspicious activity. As an example, when a credible bomb threat was made against a utility that provided power generation to the Olympic theatre, it was the ISU, working with local RCMP detachments that ultimately assessed and neutralized the threat. The immediate handling and resources allocated to protecting this utility asset resulted in an effective response. Furthermore, the resulting intelligence served to informed utilities and critical infrastructure owners across Canada about such threats and about the threat agents themselves.

Cyber-threat management was similarly developed and managed. While the vast majority of protection and response planning was focused on physical assets, collaboration and information-sharing took place in the IT environment also – an apparent first for information-sharing and planning within British Columbia and nation-wide. In the years since the 2010 Olympic Winter Games, cyber-threat management has outstripped many physical security issues related to critical infrastructure protection. This does not mean that physical threats are less than they once were, but just an indication that cyber-security planning has advanced to a new level of co-operation and priority.

Building on information from the Beijing Olympics and others, a full cyber-response center was constructed and operated for the Vancouver Olympic Games and required national, international and local industry co-operation to provide meaningful protection. Collaboration between the Olympic IT operations centre and national cyber-security programs and cyber-alerts was extremely active. While not as profound in terms of security preparation, IT risk management activities were also evident within industry's Games preparation indicating that cyber-security messaging was being taken seriously by owner/operators. Canadian and foreign cyber-security incident response centres had developed reasonable governance and communication plans and the indications were that cyber incidents were being taken seriously as part of the intelligence briefings and voluntary incident reporting during the Olympic Games.

The ISU held daily briefings for industry partners. These briefings were effective, informative and relevant. Information supplied by industry and police was included. Key Olympic sponsors, some of which had attracted global protest were included in briefings. In the spirit of full collaboration, the U.S. Overseas Security Advisory Council (OSAC) provided situational reporting before the Games and at junctures during the games, as well as providing broadcast security alerts during the Games as necessitated by various threat events and threat potential. Industry, intelligence groups and policing agencies came together in a meaningful and complex information-sharing environment and maintained confidentiality, mutual respect and accountability through the entire process.

As information was shared and analyzed, intelligence products were developed and circulated through this collaborative environment. Undoubtedly the shared information on many protest events was useful in gaining new insight into protest group tactics and activities, as well as assisting police to shut down some criminal activity during the Games. After the 2010 Winter Olympic Games, debriefs were plentiful and access to many classified reports was made possible under NRCan's classified briefing structure so that industry as a whole (not just those in British Columbia) benefited from lessons learned. There was considerable ground-breaking work and new methodologies that industry and police alike could rely on when planning for other national and international events. Significant violent protest occurred at government and industry events in eastern Canada following the Olympic Games. Lessons learned served to assist all those who participated in the protection planning and response contingencies at these events.

The E-INSET Initiative

Of particular note, in the months leading up to the 2010 Olympic Winter Games was the outreach and work of the RCMP's British Columbia Integrated National Enforcement Team (E-INSET). Specializing in outreach as a core function, E-INSET served the Olympic Games preparations by raising awareness around terrorist event planning. E-INSET developed training and awareness programs for first responders that heightened the ability of first responders to identify and report suspicious activities that could be precursors to terrorist activity. This placed hundreds more eyes in the public domain that knew their local environment and were then trained in identifying abnormal behavior. As first responders, they also received instruction about response to events like bomb threats, explosions and other life-threatening events so that they became aware of the inherent dangers associated with responding to a terrorist-based event, like secondary explosions.

In addition, E-INSET partnered with British Columbia's electricity utility to prepare a training video that spoke about terrorism from an awareness perspective. The utility provided the video and associated awareness training to its front line employees who were operating within the Olympic theatre or who had a role in the delivery of electricity along critical pathways. Through this video, employees gained perspective on the problem of and precursors to terrorist acts. The training enabled them to watch for and identify social engineering attempts, terrorist planning behavior around critical assets, and suspicious activity that indicated a departure from normal daily operations.

Developing this type of training for industry also established another trust-level relationship where policing and intelligence could be delivered in a comprehensive and useful way to industry. This E-INSET product also provided the basis for training materials to be made available to other utilities and industries elsewhere in Canada. E-INSET served to create a new model of private-public cooperation as it is applied to policing and asset protection. It demonstrated that this level of cooperation not only assists both sides of the protection and response equation, but is essential in combating terrorism and serious crime.

Future Hurdles & Lessons Learned

Lessons learned from the Olympic Games protection program seem self-evident. The ability of disparate organizations to come together, to build co-operative environments such as the one established for the Olympic Games produced desired benefits. One would have expected the Olympic program to be a framework for information-sharing on a national basis going forward. Certainly, there were numerous security and emergency management professionals involved in the Olympic Games planning process who were ready to speak positively about the experience and to encourage the development of a similar program for industry, police and intelligence communities across the country. What takes place at major events like the Olympic Games, however, often has a life of its own grown out of the excitement and energy (and funding) applied to events of this type. Lessons-learned will not necessarily be applied in the future.

With respect to the energy sector in Canada, it is clear that NRCan and the RCMP Critical Infrastructure Intelligence Team, Federal Policing Criminal Operations (and others) have come together to continue building on information sharing practices, intelligence products for industry, classified briefings, a national security incident reporting database and other essential protection programs. The recent introduction of a National Energy Infrastructure Test Centre (NEITC), a Systems Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) laboratory and training facility for industry and government is one such initiative promoted by NRCan to serve critical infrastructure protection objectives. Funding and supporting such initiatives is in the best interests of all stakeholders.

National programs like the ones sponsored by NRCan and the RCMP may not even be widely known or understood within Canadian industry by executives, risk managers and others who make policy decisions regarding industry program support. Or, those who participate in such activities as classified briefings and other training and information products may not understand the relevance or appreciate how they contribute to a national protection plan. In fact, it may be that a regional player in any sector may see their role as isolated from the national picture and are unable to draw a direct, relevant connection between what government is doing and what the local stakeholder requires. Industry players do not necessarily perceive the threat from terrorism and serious crimes to be a serious threat to local operations. It is also true that even amongst those who understand the threat potential and who support government programs, they have yet to escalate their involvement in these programs for one or more reasons.

All of this serves to make information-sharing and other forms of cooperation difficult to sustain, yet federally sponsored initiatives require demonstrated support across industry. The small number of private companies supporting these programs may indicate the need for change. Still, any program, current or future related to national security will require collaboration and information-sharing between stakeholders, as well as some form of disclosure in a trusted environment. Over time industry participation always seems to waver irrespective of program type, program initiator or program sponsor. Perhaps the question then becomes how to make programs self-sustaining. The Olympic Games demonstrated that, despite awkward beginnings, this type of environment can be created

when there is a sense of urgency. Translating this into an ongoing, national program will be more difficult without the necessary commitment from industry and government partners.

An International Perspective – 'South of the Border'

The United States takes national security extremely seriously and US industry partners are also fiercely loyal to US national security objectives. The sheer depth and breadth of American infrastructure makes their program development extremely complex, but there is every indication that information-sharing initiatives are gaining ground through groups like InfraGard and others.

Within the US, the Federal Bureau of Investigation (FBI) operates a national program called InfraGard[6] which is a "…public-private partnership between the FBI and members of the private sector who are focused on intrusions and vulnerabilities affecting 18 critical infrastructures." InfraGard membership, which is screened via background checks, is involved in the exchange of industry specific information, as well as FBI and other government reporting back to industry. InfraGard enjoys a national membership of more than 55,000 industry security professionals and boasts thousands of new membership applications each year.

Despite competing government, industry and standards-based working group programs throughout the US, there can be no doubt the FBI has developed a strong and successful public-private environment for collaboration and information-sharing. It may be of interest to Canadian authorities or researchers to review InfraGard's achievements and consider whether it has applicability to the meaningful work that is underway in Canada.
In some respects, participation in, and funding of international initiatives by Canadian companies competes with NRCan's programs. This begs the question as to whether a 'made-in-Canada solution' is important or even relevant, and if so, what it will take to create the sense of urgency necessary to develop it more extensively. It seems important that within Canada, industry needs to work with its own national partners because in times of crisis, international agencies will not have jurisdiction or immediate relevance in responding to and recovering from emergencies. The 2010 Winter Olympic Games proved that creating an appropriate security environment and working partnerships was important to success and was possible because everything needed to make it happen (the will, resources and relationships) were in place. This included international participation relating to information-sharing. The US Overseas Security Advisory Council (OSAC) provided situational reporting and broadcast security alerts as necessitated by various threat events and the threat potential during the 2010 Olympic Games.

Given that Canada and the USA share critical infrastructure and concerns, co-operative and complimentary programs are likely to provide additional benefits to both. A vibrant information-sharing network already exists between cross border police and intelligence agencies, just as industry also enjoys excellent cooperation with US and international

[6] Website at **Error! Hyperlink reference not valid.**

Associations, working groups and standards bodies. As collaboration improves, and to the extent that restrictions on the sharing of classified products on both sides of the border are eased, information-sharing initiatives are likely to lead to greater benefit to both and enhanced levels of trust. Such a future bodes well for improvements in the critical infrastructure protection programs of both countries.

Summary

Without a doubt, national security and emergency planning efforts on a national scale require a program of trusted information-sharing between government agencies and industry. The justification for such information-sharing may require ongoing reiteration, but without it we will be reduced to a model of industry-based standards for protection and response and local and national emergency responders will have to remain outside looking in when tragedy strikes. Understanding the various threats to Canadian infrastructure, as well as the motivations and capabilities of threat actors, assists protection planning. But left to itself, industry can only achieve so much and looks to the police and intelligence communities to manage national protection programs for advanced threats.

It is difficult to rally all industry partners to participate and contribute to national programs like those developed by the RCMP and NRCan for the energy sector. Despite the continuing threat from terrorism and other forms of extremist behaviors around the world and within Canada, owners/operators often have a localized vision of responsibility which fails to recognize interdependencies and the need to support and contribute to a national response for the good of all. Dependence on international associations will be no substitute for national partners and programs in times of crisis. It was well understood during the 2010 Olympic Games that industry, police, intelligence and support agencies were working to a common goal and a common outcome.

Canada's emergency planning and national security initiatives are producing excellent collaboration and co-operation between lead government agencies like NRCan with industry associations and other critical infrastructure stakeholders. Information is shared at Sector Network meetings and classified briefings. The work of the RCMP Critical Infrastructure Intelligence Team, Federal Policing Criminal Operations and the Canadian Cyber Incident Response Centre (CCIRC) in collecting information and providing information and intelligence products, continues to improve.

Although the Federal Government continues to fund these efforts, it is at a basic level and industry is not filling the gap to the extent many would wish. Collaboration and cooperation is, therefore not wide-spread despite the numerous examples of cooperation where industry and police have worked closely together to thwart attacks or respond to emergent situations. The message does not seem to be reaching industry at large: support for these programs is essential to critical infrastructure protection planning.

The following article is based on, and is a tribute to, the work of Jacques Shore, whose early research on legal obligations regarding information-sharing appeared in 2005 in a paper published by the Canadian Centre of Intelligence and Security Studies. This synopsis draws on three of his articles on the subject including the most recent (2013) which is awaiting publication. I am indebted to Jacques Shore for his permission to draw upon this body of work so that it can be included in the inaugural issue of the Infrastructure Resilience Risk Reporter (IR3). Comments and contributions to this and any other article which appears in IR3 (1) are welcomed for publication in future issues.

The Obligation to Share Information

Angela Gendron, Managing Editor

The Canadian government's moral and legal obligations with regard to the protection of critical infrastructure and resilience against disruptions is both a domestic and an international one by virtue of obligations to allies and its ratification of the North American Security and Prosperity Partnership Agreement (SPP). The SPP commits the United States, Canada and Mexico to developing and adopting a common approach to the protection of shared critical energy infrastructure (CEI). That commitment encompasses the sharing of best practices.

The Canadian government's duty to protect encompasses traditionally defined responsibilities such as defending territorial sovereignty, patrolling borders, and policing communities, as well as the critical infrastructure (CI) upon which the safety and well-being of its citizens depend. It is reasonable to assume that this obligation extends also to information infrastructure. Canada's ten critical infrastructure sectors are all cyber-dependent and significant vulnerabilities are inherent in these cyber links and the interdependencies which exist within and between sectors.[7] For example, disruption or destruction of a hydro-electric plant could well result from a cyber intrusion into its control system with a corresponding risk to public safety.

While most of Canada's critical infrastructure is owned and operated by private entities or provincial, territorial, or municipal governments,[8] the federal government retains jurisdiction over national security. Its federal mandate derives from the powers bestowed by the *Constitution Act, 1867* and in particular, the peace, order, and good government power (section 91) and the defence power (section 91(7)). While no legislation explicitly defines the precise duties of the federal government *vis-à-vis* digital threats to privately or jointly-owned (public-private) critical infrastructure, several agencies and departments – at all levels of government have issued policies, strategies, and action plans touching on cyber protection for critical infrastructure. These documents could be used to hold the Canadian government accountable for the safety of citizens and, by extension, for the uninterrupted

[7] Cf. John Adams, "The Government of Canada and Cyber Security: Security Begins at Home" *Journal of Military and Strategic Studies* , Vol. 14, No. 2 (2012), p. 13.
[8] Office of the Auditor General of Canada, *Fall 2012 Report of the Auditor General of Canada to the House of Commons, Protecting Canadian Critical Infrastructure Against Cyber Threats*, Chap. 3 (2012) at §3.26, online: <http://www.oag-bvg.gc.ca/internet/docs/parl_oag_201210_03_e.pdf > [*Auditor General's Report*].

provision of essential services. Settlements have already occurred between the public and critical infrastructure owners and the government. The Hon. John C. Major, Q.C., the Commissioner of the Inquiry into the investigation of the 1985 bombing of Air India Flight 182, expressed the view that an ex-gratia payment should be made to the families of the victims and that funding should be found to establish an academic institute for the study of terrorism – the "Kanishka Centre."

Apart from Canada's public law obligation to protect its citizens, entities in *both the public and private sectors* may face private law sanctions in the event of a cyber security breach where parties can be held responsible for failing "to reduce or eliminate risk"[9] although this has not so far been confirmed by the courts.

Shore's most recent article[10] provides a comprehensive review of the legal obligations of the public and private sectors to protect citizens. The case law he cites regarding a duty of care is a work in progress, but with regard to his focus on cyber issues, no case law imposing a duty of care to protect critical infrastructure from cyber attacks in the national security context exists. As he says, however, "it is possible to imagine a scenario in which an owner, operator, or government entity could be held liable for negligence, economic loss, breach of contract, or breach of a fiduciary duty as a consequence of failing to properly secure critical infrastructure cyber systems."

Acting in the Interests of Others

Crown immunity continues to diminish under pressure from a Canadian society which increasingly recognizes the rights of individuals who have sustained injuries as a result of the negligent acts of government. The requirements of the SPP, other international relationships and the growth of fiduciary duties, increases the obligation to volunteer beneficial information for the advantage of others with whom they have a special relationship. Nowhere is this more important than in the protection of Canada's critical infrastructure sectors which are predominantly in private ownership, geographically dispersed, significantly interdependent, and, in the case of the finance, transport, health and energy sectors, globally connected.

Although a potential strategic target for terrorists, critical infrastructure is currently sustaining a high level of cyber espionage intrusions which, when directed against industrial control systems, threaten not just the integrity and reliability of data, but the physical destruction of systems. The consequences for continuity of service and the safety and well-being of the public are potentially dire. Public-private sector arrangements in operation to safeguard sensitive infrastructure are therefore clearly a matter vital to national interests and security.

---

[9] Gideon Emcee Christian, "A New Approach to Data Security Breaches" *Canadian Journal of Law and Technology.* Vol. 7, No.1 (2009), p. 149, citing Meiring De Villiers, "Reasonable Foreseeability in the Information Security Law: A Forensic Analysis," *Hastings Communications and Entertainment Law Journal* Vol. 30, No. 3 (2008), p. 419.

[10] To be published in the International Journal of Intelligence and CounterIntelligence

Responsibility for CI is shared between the owners and operators and federal, provincial, and territorial governments.[11] At the federal level, a number of different agencies and departments are mandated to prevent, detect, and mitigate threats as well build resilience to natural hazards. However, the multiplicity of jurisdictional authorities which cross Canada and the private-public sector divide, can lead to confusion about respective responsibilities. Achieving cohesive and co-operative partnerships is, therefore, a challenge which is further complicated by the conflation of threats and risks signalled by Canada's 'all-hazards' approach to security and resilience which brings into play, as never before, emergency responders.

The duty of the Canadian government to secure CI was acknowledged in its *National Security Policy* which stated that, "addressing many of these threats [to national security] requires a coordinated approach with other key partners—provinces, territories, communities, the private sector and allies." In fact, if governments fail to pursue public-private partnerships to aid in the security of CI and this results in harm to citizens and/or industry, claims may be sustained by a finding of a neglected duty of care.

The various policies, strategies, and action plans developed by various tiers of government and agencies for the protection for CI, including information infrastructure, recognize both the responsibility of owners and operators and those of government to support them. Providing timely information, both routinely and in crisis, as well as sharing information concerning threats and vulnerabilities with industry players and intelligence agencies, is critical to the prevention and mitigation of disruptive events.

Under the second and third pillars of Canada's *Cyber Security Strategy*,[12] for example, the federal government commits to partnering with the provinces and territories to increase public awareness, and with the private sector and critical infrastructure sectors, to share information regarding existing and emerging threats, defensive techniques and other best practices.

Public sector operators of CI, once alerted to the need to share by Public Safety Canada (PSC), may have a legal imperative to work cooperatively in partnership to secure critical infrastructure and to seek assistance from PSC or risk legal liability. Private sector CI companies and agencies that fail to gather, evaluate, and/or disseminate critical information with respect to the protection of CI within the SPP partnership, may also face actions in damages. Although public regulatory standard CAN/CSA Z731-03 is voluntary, there are legal implications for government and private sector owners and operators who are not compliant.

---

[11] Public Safety Canada, *Action Plan for Critical Infrastructure* (2009), accessible at: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr/index-eng.aspx at 3 [*Action Plan for Critical Infrastructure*]. See also Public Safety Canada, *Cyber Security in the Canadian Federal Government*, accessible at http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/fdrl-gvrnmnt-eng.aspx [*Cyber Security in the Canadian Federal Government*].

[12] Public Safety Canada, *Canada's Cyber Security Strategy* (2010), accessible at ttp://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx.

Despite some federal government progress in building partnerships with owners and operators of critical infrastructure, the 2012 Report of the Auditor General[13] identified, among other deficiencies, problems relating to the sharing of information between government agencies and stakeholders. Encouraging stakeholders to exchange confidential information relating to threats, vulnerabilities and best practice is one of the most important ways to protect CI assets, networks and data yet the Auditor General noted that the government had failed to fully establish information-sharing partnerships and fora for critical infrastructure industries.

The *National Strategy for Critical Infrastructure*[14] issued in 2009 called for the creation of 10 critical infrastructure "sector networks," but only 6 had been set up by the time the Auditor General's report was completed and some of these were hardly functional.[15] These sector networks comprise private sector owners and operators of CI as well as stakeholders from all levels of government. Their aim is:

- to promote timely information-sharing;
- to identify issues of national, regional or sectoral concern;
- to use subject-matter expertise from critical infrastructure sectors to provide guidance on current and future challenges; and
- to develop tools and best practices for strengthening the resiliency of critical infrastructure across the full spectrum of prevention, mitigation, preparedness, response and recovery.[16]

Although the Auditor General criticized the delay in establishing these sector networks, the report positively singled out one sector, the energy and utilities network managed by Natural Resources Canada, as regularly meeting and engaging with stakeholders. Based on this collaboration, the Auditor General opined that when fully functional, the sector networks "can be a valuable forum for exchanging needed information to protect critical infrastructure."[17]

The Auditor General's Report made it clear that the Canadian government must do more to involve industry in a national dialogue on cyber defence especially by raising awareness and clarifying the reporting channels between owner/operators and the government of Canada. It also determined that the Canadian Cyber Incident Response Centre (CCIRC)

---

[13] Office of the Auditor General of Canada, *Report of the Auditor General of Canada to the House of Commons, Chapter 3: Protecting Canadian Critical Infrastructure Against Cyber Threats* (2012) at §3.26, accessible at: <http://www.oag-bvg.gc.ca/internet/docs/parl_oag_201210_03_e.pdf > [*Auditor General's Report*].

[14] Canada, *National Strategy for Critical Infrastructure* (2009), accessible at http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf

[15] *Ibid*, at §3.32.
[16] *National Strategy for Critical Infrastructure*, at p. 6.
[17] *Auditor General's Report,*

was hindered from providing up-to-date advice to its clients by a lack of adequate information from the Communications Security Establishment Canada (CSEC). Moreover, although initially conceived as a 24/7 service, CCIRC had not been operating on that basis.

From a legal perspective, such failures could present a liability risk to the government. If CSEC knew of a threat, but failed to relay it to CCIRC and this had resulted in a successful cyber attack on critical infrastructure, the government could theoretically be found liable for failing to take adequate action to prevent the attack. Legal tests would apply relating to foreseeable harm, a failure to take reasonable care and whether policy reasons were such as to negate the duty of care.

Under current Canadian federal law there is no requirement that private sector entities, including critical infrastructure owners and operators, share cyber security information with other organizations or government authorities.[18] This means that any disclosure of security or data breaches, or detected incidents or intrusions is strictly voluntary.[19] Legislation to require private organizations to report breaches to the Office of the Information and Privacy Commissioner if the security of personal data has been compromised has been proposed, but made no progress to date.

Private sector compliance or co-operation is also purely voluntary in the USA although recommendations to foster compliance include the possibility of legislation that would limit tort liability and cyber security insurance. Shore asserts that legislators in Canada must also establish strong incentives for organizations to protect consumer data and sensitive information from digital theft.

A key objective for both Canadian and US governments is the facilitation of information-sharing, but in both countries objections have been raised to a) any legislation requiring private sector organizations to report significant data breaches to the government; and b) the setting of minimum national cyber security standards for critical infrastructure sectors.

Shore's assessment is that Canada's current legal framework could impose duties on private and public sector actors to ensure the safeguarding of critical infrastructure including any digital components. Accordingly, a legal imperative exists for governments to proactively seek to detect and deter attacks on Canadian cyber systems, as well as for private sector owners and operators of critical infrastructure to exercise the utmost care in shielding their operational platforms and data from attack. The 2012 Report of the Auditor General, 'Protecting Canadian Critical Infrastructure Against Cyber Threats,' highlighted the gaps which still remain with respect to establishing sector networks which facilitate partnerships and information-sharing.

---

[18] Note that section 34.1(1) of Alberta's *Personal Information Protection Act*, SA 2003, c P 6.5 requires organizations to provide notice to the Information and Privacy Commissioner of certain security breaches relating to personal information.

[19] National Cyber Security Directorate, *Cyber Incident Against Telvent*, Question Period Note (February 22, 2013) released under the *Access to Information Act*. This briefing note was provided to Vic Toews, Minister of Public Safety, shortly after a security breach at a Canadian manufacturing company was reported in the media.

Conclusion

The safety of Canada's critical infrastructure is best assured by co-operation between the public and private sectors. Owners of critical infrastructure are ultimately responsible for protecting their assets and upgrading and maintaining information infrastructure, but governments also have responsibility to provide them with timely information concerning threats and vulnerabilities. Unless information is shared expeditiously between government agencies, CI owners and operators and other players, the goal of prevention, preparation, mitigation and rapid recovery from all hazards is unlikely to be achieved.

Shore asserts not only that there is "strong evidence to suggest that a legal duty to act exists, [but] a moral imperative lies with the government to take the necessary steps to protect its citizens from the threats of the current digital age and the potentially tragic consequences of a sinister cyber attack. He argues that "political accountability to Canadians, demands nothing less."

While the government must properly fund, promote, and support security and resilience initiatives, particularly those which aim to improve information-sharing among all partners including emergency response teams, private sector actors need to engage actively in them too. Due diligence grounds may not provide exemption from a duty of care with respect to information-sharing in circumstances in which parties can be held responsible for failing "to reduce or eliminate risk."

Achieving effective, nationwide protection of Canada's most sensitive infrastructure will require central co-ordination and facilitation, the active participation of multiple stakeholders, sufficient funding and investment, and consistent political leadership and commitment. Following Shore's reasoning, an enhanced sense of moral responsibility to others and greater legislative support will also be needed.

Literature Corner

The following is intended to provide interested readers with articles and sources on topics of professional interest

Books

"Reducing Vulnerability of Critical Infrastructures"

ISBN9782553015977 Editor Presses Internationales Polytechnique. 68 Pages Published 2011-08-25 Paperback $22.95
http://www.presses-polytechnique.ca/en/reducing-vulnerability-of-critical-infrastructures

Authors Luciano Morabito, Benoît Robert

Synopsis of Publisher's Overview:

Critical infrastructures are systems that provide the basic resources society requires, such as drinking water, transportation, telecommunications and energy. These resources are used by the population, but also by other critical infrastructures. Given the high level of interdependence between critical infrastructures, failure of a single element can cause a domino effect with negative consequences for all other critical infrastructures and therefore the population. The potentially dramatic consequences of such failures have been highlighted by recent catastrophic situations, both at the national - the 1998 ice storm in southern Quebec - and international levels - the earthquake-related Fukushima Daiichi nuclear disaster in Japan in March 2011.

"Reducing Vulnerability of Critical Infrastructures" is a book primarily aimed at municipal risk managers, government services and essential services suppliers, but also offers academics and students in management and engineering a new theoretical approach to risk. It results from years of collaboration between multiple public and private partners. It offers a concrete methodology for identifying and assessing interdependencies between critical infrastructures using a flexible mapping approach that allows managers to locate their infrastructures more or less precisely depending on the degree of confidentiality they wish to preserve. This allowance cleverly circumvents problems associated with the sharing of confidential data. The approach is based on the consequences of failures rather than their causes.

Occasional Papers: Priority Issues / Étude hors-série: questions prioritaires
Canadian Security Intelligence Service / Service canadien du renseignement de sécurité

Assessing Cyber Threats to Canadian Infrastructure/Évaluation Des Cybermenaces Pesant Contre Les Infrastructures Du Canada

By Angela Gendron & Martin Rudner
https://www.csis.gc.ca/pblctns/ccsnlpprs-fra.asp

Article Abstracts

"Information-sharing and collaboration for critical infrastructure resilience - a comprehensive review on barriers and emerging capabilities."

Among authors, researchers and government agencies, information-sharing and collaboration have been recognized as a critical issue for improving crisis response effectiveness and efficiency, since no single organisation has all the necessary resources, possesses and relevant information or owns expertise to cope with all types of extreme events. This work presents a review study on general issues and barriers to information-sharing and collaboration during critical infrastructure (CI) crisis response. Emerging concepts and capabilities that are promising for making an improvement in the field are also presented and discussed. Possible contribution to CI protection and resilience (CIP/R) is discussed concerning the importance of matching organisational structure characteristics, technological capabilities and sociological influence. The needs and opportunities for future research are also highlighted, emphasising the need for a comprehensive framework of analysis and deployment.

Boris Petrenj; Emanuele Lettieri & Paolo Trucco, *International Journal of Critical Infrastructures*, Vol.9, No.4 (2013)
http://www.inderscience.com/info/inarticle.php?artid=58171

Abstract:

"Resilience of civil infrastructure systems: literature review for improved asset management."

Infrastructure resilience has drawn significant attention in recent years, partly because the occurrence of low-probability and high-consequence disruptive events like Hurricane Katrina, the Indonesian tsunami, 9/11 and others. Since civil infrastructure systems support society's welfare and viability, continuous infrastructural operation is critical. Along protection approaches, resilience concepts support achievement of near-continuous infrastructure operation. A variety of frameworks, models, and tools exist for advancing infrastructure resilience research. Nevertheless, translation of resilience concepts into practical methodologies for informing civil infrastructure operation and management remains challenging. This paper presents a state-of-the-art literature review on civil infrastructure resilience, particularly water distribution systems, enabling practical

applications of infrastructure resilience towards improved system management. The literature review has two stages, quantitative and qualitative. Infrastructure resilience is defined to provide a foundation for operationalization of infrastructure resilience concepts, enabling the inclusion of practical resilience considerations in formal management systems such as infrastructure asset management systems.

Leon F. Gay & Sunil K. Sinha, *International Journal of Critical Infrastructures*, Vol.9, No.4 (2013)http://www.inderscience.com/info/inarticle.php?artid=58172

Homeland Security Affairs
http://www.hsaj.org/
Vol. 9, 2013

"Supply Chain Resilience: Diversity + Self-organization = Adaptation"
By Philip Palin

"The Two Faces of DHS: Balancing the Department's Responsibilities"
By Jerome H. Kahan

"The Plan, Type, Source, Report Cycle: A Unifying Concept for National Guard Preparedness"
By David W. Smith

"Entrepreneurial Security: A Free-Market Model for National Economic Security"
By Shawn F. Peppers

"Enabling Public Safety Priority Use of Commercial Wireless Networks"
By Ryan Hallahan & Jon M. Peha

"There's a Pattern Here: The Case to Integrate Environmental Security into Homeland Security Strategy"
By James D. Ramsay & Terrence M. O'Sullivan

"Ending America's Energy Insecurity: Why Electric Vehicles Should Drive the United States to Energy Independence"
By Fred Stein

International Journal of Critical Infrastructures

http://www.inderscience.com/jhome.php?jcode=ijcis

Vol. 9 No. 4 (2013)

"Simulation and anticipation of domino effects among critical infrastructures"
By Robert Benoît, Luciano Morabito, Cédric Debernard
"Information sharing and collaboration for critical infrastructure resilience - a comprehensive review on barriers and emerging capabilities"
By Boris Petrenj, Emanuele Lettieri, Paolo Trucco

"Resilience of civil infrastructure systems: literature review for improved asset management"
By Leon F. Gay, Sunil K. Sinha

"Seismic protection of critical infrastructures through innovative technologies"
By R. Sreekala, N. Gopalakrishnan, K. Muthumani, K. Sathishkumar, G.V. Rama Rao; Nagesh R. Iyer

International Journal of Cyber Warfare and Terrorism
http://www.igi-global.com/journal/international-journal-cyber-warfare-terrorism/1167

Vol. 3, Issue 1 (2013)

"Intellectual Property Systems in Software"
By Ricardo Rejas-Muslera, Elena Davara, Alain Abran, Luigi Buglione

"On the Study of Certified Originality for Digital Alteration Problem: Technology Developments of the Time Authentication "
By Masakazu Ohashi & Mayumi Hori
In our modern clock-ruled culture, it is not too much to say that no society can exist

"Intellectual Property Protection in Small Knowledge Intensive Enterprises"
By Riikka Kulmala & Juha Kettunen

"Online Interaction with Millenials: Institution vs. Community"
By Kurt Komaromi, Fahri Unsal, G. Scott Erickson

Journal of Applied Security Research

http://www.tandfonline.com/toc/wasr20/current#.UtgwEPuFeuI
Volume 9, Issue 1, 2014

"Who Skips? An Analysis of Bail Bond Failure to Appear"
By Brian Johnson, Christopher Kierkus & Christine Yalda

"Effects of Cultural Collectivism on Terrorism Favorability"
By Daniela Peterka-Benton & Bond Benton
pages 17-40

"Attitudes of Private Security Officers in Singapore Toward Their Work Environment"
By Sylvia S. L. Lim & Mahesh K. Nalla
pages 41-56

"Negotiating in the 21st Century: Bridging the Gap Between Technology and Hostage Negotiation"
By James Nichols

"Terrorism and Chemical Security: Small Quantities of Chemicals of Interest"
By Maria Dewing

"The Bioterrorism Act and Water Utilities Protection: How to Proceed from Policy to Practice"
By Frank Cinturati

Journal of Homeland Security and Emergency Management

http://www.degruyter.com/view/j/jhsem

Volume 10, Issue 2 (Oct 2013)

"Impact of Providing Real-Time Traffic Information on No-Notice or Short-Notice Evacuation Efficiency – A Case Study"
By Yuanchang Xie, Tugba Arsava, Chao Zhang

"Compliance of Community Hospitals with the Chemical Facility Anti-Terrorism Standards (CFATS) in the Western United States"
By Morgan M Bliss,. Kiril D Hristovski,. Jon W. Ulrich

"Analysis of Criminal and Terrorist Related Episodes in Railway Infrastructure Scenarios"
By Francesca Cillis, Maria Carla De Maggio, Concetta Pragliola, Roberto Setola

GIS in Emergency Management Cultures: An Empirical Approach to Understanding Inter- and Intra-agency Communication During Emergencies"
By Joseph J Breen,. David R Parrish.

"Catastrophe Characteristics and their Impact on Critical Supply Chains: Problematizing Materiel Convergence and Management Following Hurricane Katrina"
By Tricia Wachtendorf, Bethany Brown, Jose Holguin-Veras

"Options and Challenges of a Resilience-Based, Network-Focused Port Security Grant Program"
By Eric Taquechel

"Incorporating Time Dynamics in the Analysis of Social Networks in Emergency Management"
By Jeroen Wolbers, Peter Groenewegen, Julia Mollee, Jan Bim

"Death Modes from a Loss of Energy Infrastructure Continuity in a Community Setting"
By Athol Yates
Page 587
Published Online: 09/24/2013

"Businesses and International Security Events: Case Study of the 2012 G8 Summit in Frederick County, Maryland"
By Mark R. Landahl
"First Responder Knowledge and Training Needs for Bioterrorism"
By Heather C. Galada, Patrick L. Gurian, Tao Hong,

Resilience
International Policies, Practices and Discourses
http://www.tandfonline.com/toc/resi20/current#.Utg2YfuFeuJ

Volume 1, Issue 3, 2013

"The nature of resilience"
By Chris Zebrowski

"The empirical falsity of the human subject: new materialism, climate change and the shared critique of artifice"
By Jessica Schmidt

"Hidden transcripts of resilience: power and politics in Jamaican disaster management"
By Kevin Grove

"Resilience, normativity and vulnerability"
By Robin May Schott

"From security to resilience? (Neo)liberalism, war and terror after 9/11"
By Ben Whitham

"Water"
By Henry Vaux

"Disaster resiliency – interdisciplinary perspectives"
By Susan Kinnear

****