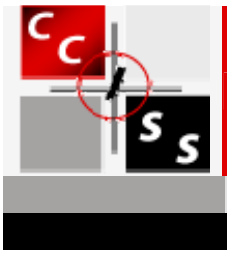

THE CANADIAN CENTRE OF INTELLIGENCE
AND SECURITY STUDIES
AT CARLETON UNIVERSITY

CCISS

Critical Energy Infrastructure Protection
Policy Research Series

THE LEGAL IMPERATIVE TO PROTECT CRITICAL ENERGY INFRASTRUCTURE

Jacques J.M. Shore

No. 2 – 2007-2008
March, 2008

This study is undertaken as part of the CCISS Critical Energy Infrastructure Protection Policy Research Project supported by a Contribution Agreement with Natural Resources Canada, Energy Infrastructure Protection Division

The Legal Imperative to Protect Critical Energy Infrastructure

Jacques J.M. Shore*

I. INTRODUCTION:

The terrorist actions of September 11, 2001, highlighted the threat to Canada's national and economic security. Canada's Critical Infrastructure (CI), often considered a strategic target for terrorists, consists of physical and information technology facilities, networks, services and assets. CI is crucial to the health, safety, security and prosperity of Canadians because it underpins every sector of society and the economy providing all the basic services upon which Canadians depend.

Canadian CI is made up of a number of sectors that include energy and utilities, communications and information technology, finance, health care, food, water, transportation, government, and manufacturing. These CI sectors face a range of physical and cyber threats that include terrorism, natural phenomena such as earthquakes, floods, or ice storms, accidents and cyber-attacks. Given the highly connected and highly interdependent nature of these national CI sectors, failures or disruptions in one or more infrastructure systems can cascade through other systems, causing unexpected and serious failures of essential services.

In fact, poor arrangements to prevent disasters and respond appropriately to tragic events could have potentially devastating implications for Canadians. The large power outage that swept across much of Ontario and the northeastern United States on August 14, 2003, provided an objective lesson in energy infrastructure interdependencies by demonstrating how a disruption in one infrastructure can cascade across others.

In February 2006, al-Qaeda called again for terror attacks on North American oil fields, pipelines, loading platforms and carriers. In this call, Canada was specifically targeted.[1] A recent Conference Board of Canada report entitled, *Facing Risks: Global Security Trends and Canada*[2], reiterated that Canada is vulnerable to attacks on energy infrastructure aimed at disrupting service to the United States. Given that Critical Energy Infrastructure (CEI) is of paramount importance to the economy of Canada, making a

---

* Jacques J.M. Shore is a partner in the Advocacy and Government Relations Practice Group at the Ottawa Office of Gowling Lafleur Henderson LLP. The author is grateful to Chris Schafer, associate in the Advocacy and Government Relations Practice Group at the Ottawa Office of Gowling Lafleur Henderson LLP, for his contribution in the researching and preparation of this paper. Please note that this paper is not intended to serve as a legal opinion but is designed to provide the views of the author.

[1] Adeeb al-Bassam, "Bin Laden and the Oil Weapon" 30:1428 Sawt al-Jihad (2006) 28. Text transcribed and translated by the SITE Institute.

[2] Conference Board of Canada, *Facing Risks: Global Security Trends and Canada* (Ottawa: Conference Board of Canada, 2006).

substantial contribution to national income, employment, economic activity, exports and growth, protecting CEI is crucial.

Ultimately, protecting national security, which encompasses CEI security, is a task for which government has primary responsibility. It is the role of government to do its utmost to protect its citizens, however it cannot do so by itself. To a great extent, this is because many potential terrorist targets, such as electrical power, natural gas, oil production and transmission systems, are owned and/or operated by the private sector. To foster and help establish a "secure economy"[3], government and the private sector have mutually important roles to play.

Beyond the motivation to reduce threats to national and corporate security that both public and private sectors must share, another motivation in "securing the economy" is to guard against legal liability. In order to avoid or reduce potential legal liability, there is a legal imperative on the part of both government and private enterprise to protect CEI.

II. THE RESPONSIBILITY OF GOVERNMENT TO PROTECT CEI

The most primary and fundamental responsibility of government is the protection of its citizenry. The *National Security Policy* of Canada states that, "There can be no greater role, no more important obligation for a government, than the protection and safety of its citizens."[4] This was confirmed by the Supreme Court of Canada in the recent *Charkaoui* decision.[5] The fulfillment by government of its commitment to national security cannot be achieved without the protection of Canada's CEI.

CEI, such as electrical power (generation, transmission, and nuclear), natural gas, and oil production and transmission systems, are integral to the safety, security, and prosperity of all Canadians. Canadians require assurance that CEI is viable and resilient to disasters and terrorist attacks. Regardless of who owns or operates the CEI, Canadians expect it to continue to function and they expect government to play a leadership role in ensuring this happens. The foundation of this responsibility on the part of government to protect CEI from the various threats it faces, rests with the commitment to "Peace, Order and good government" in the *Constitution Act, 1867*.

Government action towards assuring a resilient and survivable CEI protects the lives and livelihoods of Canadians by ensuring their physical and economic safety and security. In Canada, a complex industrial society, direct and indirect dependencies on government have been widely and deeply entrenched such that citizens have come to require the functions of government in their day-to-day lives. In the case of threats to CEI, which are

---

[3] Deloitte Touche Tohmatsu, *Prospering in the Secure Economy* (Switzerland: Deloitte Touche Tohmatsu, 2005).

[4] Canada, Privy Council Office, *Securing an Open Society: Canada's National Security Policy* (Ottawa: Privy Council Office, 2004) at vii.

[5] *Charkaoui v. Canada (Citizenship and Immigration)*, [2007] 1 S.C.R. 350 at para. 1. The Chief Justice on behalf of the Court states that "One of the most fundamental responsibilities of a government is to ensure the security of its citizens."

beyond the capacity of individuals and corporations to address alone, a response by government is expected and needed. The obligation to ensure adequate CEI security planning and preparation rests with government.[6]

In a globalized world made interconnected and interdependent by advances in information technology, transportation, and telecommunications, Canada is not immune to events occurring outside its borders. This is why the federal government, through Public Safety Canada (PSC), established the *National Critical Infrastructure Assurance Program* (*NCIAP*). According to PSC, "The NCIAP is an ongoing collaboration between private sector partners and federal, provincial and territorial governments. The goals of these partnerships are to provide a national framework for cooperative action and to build a resilient national critical infrastructure."[7]

Based on the work begun under the *NCIAP*, the Government of Canada issued a *Position Paper on a National Critical Infrastructure Protection Strategy* (*NCIPS*). The Paper was developed as a result of dialogue with stakeholders on concepts and issues surrounding the development of the *NCIAP*. Consultations with private industry leaders representing Canadian CI sectors as well as various federal, provincial and municipal governments responsible for CI protection, to develop Canada's *NCIPS* began in May of 2005.

The mission of the *NCIPS* is "To create an integrated and forward-looking…strategy that will include voluntary participation from industry stakeholders as well as from federal, provincial and territorial governments."[8] The desired outcome of this strategy is that national CI will be "sufficiently resilient, thereby assuring the continued availability of essential services to Canadians."[9] The guiding principles of the strategy include awareness of the need to protect national CI among senior managers in industry and at all levels of government, and integrating physical and cyber security issues into emergency management programs. In addition, the guiding principles of the *NCIPS* also include encouraging broad participation of industry stakeholders and federal, provincial and territorial governments, and providing accountability to Canadians through legislation, regulation, policy, and due diligence for the safeguarding of national CI assets and ensuring the viability of national CI services.

---

[6] Under section 3 of the federal *Emergency Management Act*, "The Minister [of Public Safety and Emergency Preparedness] is responsible for exercising leadership relating to emergency management in Canada by coordinating, among government institutions and in cooperation with the provinces and other entities, emergency management activities." Provincially, in Ontario for example, the provincial *Emergency Management Act* is the legislative authority for emergency management in the province. Through the Ministry of Community Safety and Correctional Services, Emergency Management Ontario is responsible for promoting, developing, implementing and maintaining emergency management programs throughout Ontario.

[7] Canada, Public Safety and Emergency Preparedness Canada (PSEPC), *National Critical Infrastructure Assurance Program* (Ottawa: PSEPC, 2002), online: <www.publicsafety.gc.ca/prg/em/nciap/index-eng.aspx>.

[8] Canada, PSEPC, *Government of Canada Position Paper on a National Strategy for Critical Infrastructure Protection* (Ottawa: PSEPC, 2004) at 6.

[9] *Ibid*.

Likewise, *The Chemical, Biological, Radiological and Nuclear Strategy of the Government of Canada* (*CBRNS*) supports the government's *National Security Policy*. The aim of the *CBRNS* is to "protect Canada and Canadians by taking all possible measures to prevent, mitigate and respond effectively to a potential CBRN incident."[10] Consistent with the *CBRNS*, following the events of 9/11, the Canadian Nuclear Safety Commission (CNSC) undertook an emergency review of nuclear security and an evaluation of existing *Nuclear Security Regulations*. This broad review by the CNSC led to amendments to the *Nuclear Security Regulations* in late 2006. The amendments codified the requirements of two emergency CNSC orders of 2001, in addition to other security requirements for licensees. For example, the additional security requirements included the construction of physical protections and vehicle barriers and access control systems at nuclear power facilities.[11]

However, Canada still lags behind with respect to the protection of CI, including CEI. According to Dr. Joe Varner, "Other than defining critical infrastructure, setting up an office, and perhaps compiling a target list, Canada has done virtually nothing to protect its critical infrastructure."[12] Furthermore, "In Canada today, there is no framework at the national level to link the federal government with CIs, although a draft strategy has been under development by Public Safety Canada for several years."[13] According to the Standing Senate Committee on National Security and Defence, "The government's commitment to develop a critical infrastructure policy is a step forward, as is its publication of the position paper. The works needs to be completed quickly."[14]

Moreover, according to Dr. Martin Rudner, founding Director of the Canadian Centre of Intelligence and Security Studies:

> CEIP [Critical Energy Infrastructure Protection] across the various North American jurisdictions [including Canada] thus remains essentially defensive, emphasizing emergency preparedness, assurance, and mitigation management. A defensive posture is procedurally passive and tactical, rather than strategic and proactive…This passive, defensive orientation has tended to impede

[10] Canada, PSEPC, *The Chemical, Biological, Radiological and Nuclear Strategy of the Government of Canada* (Ottawa: PSEPC, 2005) at 3.

[11] For a more fulsome discussion of the response by the CNSC to the events of 9/11, see Gerry Frappier & David Sachs, "Security in the Nuclear Industry" (2007) 2:1 Frontline Security 14, online at <www.nuclearsafety.gc.ca/eng/newsroom/articles/2007-04-18_nuclear_safety.cfm>.

[12] Dr. Joe Varner, "Is There a Terrorist Threat to our Critical Infrastructure?" (2007) 2:1 Frontline Security 7 at 10.

[13] Stuart Brindley, "We're in this together! Critical Infrastructure: The Need for Partnership" (2007) 2:1 Frontline Security 11. Likewise, according to Dr. Martin Rudner, gaps remain in Canada's policy framework with respect to dealing with threats to national CI. Dr. Rudner points to the fact that the Canadian government does not possess a centralized clearinghouse for information relating to CEI protection for its own departments and agencies, or for sharing with our jurisdictions. See Martin Rudner, "Protecting North America's Energy Infrastructure Against Terrorism" (2006) 19 International Journal of Intelligence and CounterIntelligence 424 at 436.

[14] Standing Senate Committee on National Security and Defence, *Canadian Security Guide Book 2005 Edition: An Update of Security Problems in Search of Solutions* (Ottawa: Standing Senate Committee on National Security and Defence, 2004) at 230.

> the formation of partnerships—domestically with subnational jurisdictions and with the private sector, as well as internationally. Ultimately, a defensive, passive, tactical approach to CEIP Policy will, in effect, constrain the building of national capacity to address the contemporary threat environment.

Canada's *National Security Policy* states that, "National security deals with threats that have the potential to undermine the security of the state or society." This state-centric approach reflects the federal government's primary responsibility for the emergency management of national CI, including CEI. The Canadian government also recognizes that "Addressing many of these threats [to CEI] requires a co-ordinated approach with other key partners—provinces, territories, communities, the private sector and allies." Given that CEI is the fuel for Canada's economy that is responsible for maintaining the quality of life that Canadians enjoy, if the government fails to secure CEI or to pursue public-private partnerships to facilitate the protection of CEI by private enterprise, which results in harm being brought upon citizens and/or industry, claims may be sustained against the government by findings of a neglected duty of care.

III. REDUCING GOVERNMENT LIABILITY: THE LEGAL IMPERATIVE TO PROTECT CEI

The protection of CEI is increasingly a legal obligation of government. Federal legislation passed since 9/11 creates national security related obligations for a number of government institutions. For example, section 6 of the federal *Emergency Management Act* provides that each Minister accountable to Parliament for a government institution is to identify the risks that are within or related to his or her area of responsibility, including those related to CI, and in accordance with the policies, programs and other measures established by the Minister of Public Safety and Emergency Preparedness, prepare emergency management plans, maintain, test and implement those plans, and conduct exercises and training in relation to those plans.

With respect to liability of Canadian governments for negligence under tort law, the following elements must be proven by a plaintiff suing the government: The defendant government owed a duty to the injured party (plaintiff); by failing to exercise a degree of care based on the standard of what a reasonable person would do in a like circumstance, the government breached its duty of care; the breach of duty proximately caused an injury to the plaintiff; and, the plaintiff's injuries are significant enough to warrant compensation from the government.

The Supreme Court of Canada decisions as *Nielson v. Kamloops*[15] and *Just v. British Columbia*[16], established that government actors are not liable in negligence in tort claims for policy decisions, but only operational decisions. The basis of this immunity is that policy is the prerogative of the elected Legislature, although a government actor may be liable in negligence for the manner in which it executes or carries out a policy.

[15] [1984] 2 S.C.R. 2.
[16] [1989] 2 S.C.R. 1228.

In addition, Canada has legislatively waived their Crown immunity to certain civil actions filed by citizens seeking to recover damages caused by the negligence of the government and/or its servants.[17] Crown immunity will likely continue to diminish as the Courts increasingly recognize the rights of individuals who have sustained injuries as a result of the negligent acts of government. According to Nicholas Woodfield, a legal expert on tort liability, the common law in relation to Crown tort liability will "continue to evolve in an effort to better reflect the contemporary social, political, and economic values peculiar to each dynamic society,"[18] perhaps especially in a post 9-11 society because the threats to CEI are much more evident.

As noted above, Canada does not currently have a partnership framework in place to link the federal government with CEI owners/operators to integrate protection related activities across all critical energy sectors. According to Stuart Brindley:

> Without a recognized partnership framework in place, government and the CI sectors will not be able to effectively coordinate efforts to ensure secure, safe and reliable critical infrastructure services. This is not only a matter of national interest—it is necessary to meet the commitments we have made with our neighbours through the Security and Prosperity Partnership [SPP] of North America.[19]

On March 31, 2006, the three leaders of North America reached an agreement to advance the agenda of the SPP, part of which includes developing a common approach to shared critical infrastructure protection in mutually agreed priority areas (i.e. electricity generation and distribution, oil and gas pipelines, dams, and nuclear). An initiative under this shared approach to CEI protection is to facilitate among governments and CEI operators, the sharing of best practices.

Consequently, because of the requirements of the SPP for example, or because of the growth of fiduciary duties that require persons to act in the interests of others with whom they have a special relationship, there is an increasing obligation to volunteer beneficial information for the advantage of others.[20] Private sector CEI-related companies must have enough information to make sensible risk assessments on which to base their planning and allocate their resources. Governments and their agencies that fail to gather, evaluate, and/or disseminate critical information within a partnership framework to the private sector with respect to the protection of CEI may face actions in damages.

Likewise, public sector operators of CEI put on notice by the federal government through PSC may have a legal imperative to work cooperatively in partnership to secure CEI.

---

[17] Nicholas W. Woodfield, "The Policy/Operational Dichotomy in Intra-State Tort Liability: An Example of the Ever-Continuing Transformation of the Common Law" (2003) 29:1 Denv. J. Int'l L. & Pol'y 27 at 28. See *e.g.* the *Crown Liabilities and Proceedings Act*, R.S., 1985, c. C-50.

[18] *Ibid*.

[19] Brindley, *supra* note 13 at 13.

[20] Philip Osborne, tort law professor at the University of Manitoba, has pointed out that a significant growth in respect of tort-based legal liability for the gathering, evaluation, and communication of information is likely in the future. See Philip H. Osborne, *The Law of Torts* (Toronto: Irwin Law, 2000) at 387.

Those public sector CEI operators unable to adequately secure their facilities may also have a duty to seek assistance from PSC in partnership or risk legal liability.

According to Whitley et al., "The certainty of future terror-related lawsuits underscores the need for established 'homeland security' standards and best practices."[21] For starters, federal government policy and strategies such as its National Security Policy and the aforementioned *NCIPS* currently under development, provide convenient standards of care, and as such, are attractive tools for courts to use in resolving emergency management-based litigation.

Equally, if not more attractive, is the Canadian Standards Association's Emergency Preparedness and Response standard, (CAN/CSA Z731-03), in place since November 2003.[22] This standard provides advice on planning, administration, training, resource utilization, auditing, and other aspects of emergency preparedness and response. The standard assists public organizations, as well as businesses, develop an emergency plan to minimize the consequences of an emergency, by establishing minimum criteria for an effective approach to an emergency for organizations affected by natural, technological, and human events, such as terrorist attacks.

While CAN/CSA Z731-03 is voluntary, government CEI owners and operators, not to mention private sector CEI owners/operators, are well advised to become certified as compliant with this standard. Failure to do so could have legal implications because if CEI is attacked by terrorists resulting in the loss of life, the success or failure of a subsequent lawsuit will likely hinge on the level of security and emergency preparedness undertaken by the government owner/operator. If the defendant government is not at a minimum CAN/CSA Z731-03 compliant, plaintiffs may possess a better chance of succeeding in their claims under negligence focused tort law. In this hypothetical scenario, plaintiffs would likely claim that the defendant government knew, or at the very least ought to have known that the risk of terrorism or a natural disaster to CEI was high, and consequently, the failure to implement the security and emergency management safeguards defined by CAN/CSA Z731-03 was unreasonable and a breach of a statutory or common law duty of care.

Given this reality, governments in Canada should not take lightly the emerging body of case law in the United States that suggests that inadequate counter-terrorism practices could be deemed negligent in light of reasonably foreseeable risks. In 1993, terrorists exploded a truck bomb in a parking garage basement of the World Trade Center. Victims of that attack sued the New York and New Jersey Port Authority for negligent security practices.[23] In a procedural decision in favour of the plaintiffs, the lower court found that, "in the early 1980s, the Port Authority was aware of terrorist activities occurring in other

[21] Joe D. Whitley et al., "Homeland Security, Law, and Policy Through the Lens of Critical Infrastructure and Key Asset Protection" 47 Jurimetrics J. 259 at 275.
[22] Canadian Standards Association, "Emergency Management", online: <http://www.csa.ca/standards/community_safety/default.asp?load=communitysafety&language=english>.
[23] In re World Trade Center Bombing Litig., 776 N.Y.S.2d 713 (Sup. Ct. 2004), offd, 784 N.Y.S.2d 869 (App. Div. 2004).

areas of the world, and that the WTC [World Trade Center], as a highly symbolic target, was vulnerable to terrorist attack."[24] The lower court cited the internal reports and studies of the Port Authority itself in order to demonstrate that it knew that the World Trade Center was susceptible to terrorist attack.

Given the above noted evidence, the court held that, "the Port Authority's claim that this bombing was unforeseeable as a matter of law strains credibility."[25] On appeal, a New York state appeals court unanimously affirmed the lower court's procedural findings, which enabled the case to proceed to trial.[26] On October 26, 2005, a New York jury held the Port Authority liable for neglecting to maintain adequate security practices.[27]

In Canada, recent national security related litigation against the government concerning Severe Acute Respiratory Syndrome (SARS) highlights the potential legal liability governments in Canada may face for their alleged negligence.[28] Several legal proceedings arising out of the SARS outbreak in Toronto in 2003 have been commenced and are under case management by Justice Cullity of the Ontario Superior Court of Justice.[29] In essence, Justice Cullity is being asked to consider a matter that ultimately hinges upon whether government officials who make mistakes can be made accountable to the public and victims where it can be shown that a reasonable duty of care is not exercised.

In *Abarquez v. Ontario*[30], one of the proceedings under case management, the Ontario Nurses' Association is suing the Ontario government on behalf of the Lin family and 52 other nurses for negligence in the handling of the SARS outbreak, arguing public officials failed to provide adequate and timely information alerting nurses on how to protect themselves. Although an application by the Crown for an order striking the statement of claim was allowed in part, the Court held that the negligence claims were not struck as a whole because it was not plain and obvious the plaintiffs could not succeed at trial in proving proximity between the nurses and the government. As such, the Court allowed the claim with respect to allegations that the government acted with improper motives in

[24] *Ibid*. at 718 (Order granting in part and denying in part defendant's motion for summary judgment).
[25] *Supra* note 21 at 274.
[26] In re World Trade Center Bombing litig., 784 N.Y.S.2d 869, 869 (App. Div. 2004).
[27] Anemona Hartocollis "Port Authority Found Negligent in 1993 Bombing" *N.Y. Times* (27 October 2005), A6.
[28] Although the Ontario Court of Appeal case re *Eliopoulos v. Ontario (Minister of Health & Long Term Care*, [2004] O.J. No. 3035, with respect to the more than 40 families that sued the Ontario government alleging negligence in dealing with the West Nile Virus epidemic in 2002, was dismissed by the Court for disclosing no cause of action against the Ontario government, the Court held at paragraph 25 that, "the plan falls well short of the sort of policy decision to do something about a particular risk that triggers a private law duty of care to implement such policy at the operational level in a non-negligent manner." This leaves the door open to cases in the future where government plans, amounting to an operational plan, with commensurate duties, can ground a claim by a citizen(s) against the government for the negligent implementation of a policy at the operational level. This decision was appealed to the Supreme Court of Canada, where leave to appeal was dismissed: *Eliopoulos v. Ontario (Minister of Health & Long-Term Care*, [2006] S.C.C.A. No. 514.
[29] See, *e.g., Abarquez v. Ontario*, [2005] O.J. No. 3504 and *Williams v. Attorney-General of Canada et al.*, [2005] O.J. No. 3508.
[30] *Ibid*.

terminating protective requirements in the interest of attracting tourists back to Toronto, to proceed to trial. In the future, undoubtedly litigation lawyers will seek to establish further foundations for legal liability in this area, based on negligent failure to adequately anticipate and prepare for reasonably foreseeable risks.

As such, the above cases demonstrate the following principles: inadequate counter-terrorism practices by the government may be deemed to be negligent in light of what are now surely reasonably foreseeable terrorism-related risks in a post 9/11 world, and neglect by government of its emergency management related responsibilities by taking actions that harm the public, may lead to claims being sustained against it by a finding of a neglected duty of care. Likewise, if a government or agency of government fails to take action to aid in the security of citizens in preventing or minimizing cascading damages from a terrorist attack on CEI, and preventing harm upon citizens and/or industry, claims may be sustained by a finding of negligence. This appears to make it imperative for governments, especially the federal government, that CEI public-private partnerships be established, sustained, and effective for the purposes of protecting Canadians and others who may be affected.

IV. REDUCING CORPORATE LIABILITY: THE LEGAL IMPERATIVE TO PROTECT CEI

In a large scale terrorist attack or natural disaster, governments on their own, do not possess the capability of responding fully and effectively in the aid of citizens they were elected to protect. The challenges posed in strengthening and securing CEI protection exceed the capacity of any one level of government. Since most of the CEI in modern industrial economies like Canada is privately owned and operated, the private sector has significant responsibility for the security of Canada's economy and society.

The CEI sector bills consumers proportionally to services or products consumed. Electrical power companies bill by the kilowatt. Under this model, electrical power companies cease to make money when services or consumables stop flowing to customers. Thus:

> Continuity of operations already has its own built-in motive—the more reliable the operation, the more money received…The only thing more expensive than critical infrastructure protection is loss of continuity of operations…Hurricane Katrina not only damaged much of the infrastructure of New Orleans, it also forced Entergy (the regional power company) to the brink of bankruptcy."[31]

Consequently, the profit motive of corporations encourages them, in theory, to invest in security for their CEI in order to ensure continuity of operations.[32] However, if this is not motivation enough, the threat of possible litigation ought to be sufficient.

[31] Ted G. Lewis & Rudy Darken, "Potholes and Detours in the Road to Critical Infrastructure Protection Policy" (2005) 1:2 Homeland Security Affairs 1 at 8.

Corporations have a responsibility to shareholders and employees to protect corporate assets from the more usual threats of theft, vandalism, and hackers. Post 9/11, terrorism has also been added to this list of known threats. Corporate officers and directors also have a legal duty of care to their corporation. In the event of a security breach, terrorism related or not, tort liability may ensue if investments in security were not made that might have reasonably prevented or mitigated any damages. It goes without saying that, "Inaction is a decision, and inaction can be considered negligence!"[33]

Those private sector CEI owners/operators put on notice by government through governmental national security related strategies, may have a legal imperative to work cooperatively in partnership to secure CEI, if not solely to reduce liability in the wake of a terrorist attack. Moreover, those CEI owners/operators unable to adequately secure their facilities may also have a duty to seek government assistance in partnership or risk legal liability.

CEI owners and operators who fail to implement security measures may be held liable for ignoring a recognizable danger, based upon knowledge of the existing facts, and some reasonable belief that harm may possibly follow. This proposition flows from a recent United States District Court decision wherein Judge Alvin Hellerstein refused to release Boeing Corporation from liability in the 9/11 terrorist attacks. The judge held that, "…it was reasonably foreseeable that a failure to design a secure cockpit could contribute to a breaking and entering into, and take-over of a cockpit by hijackers or other unauthorized individuals…"[34] This ruling suggests the potentiality that CI sector owners and operators may be held legally liable for damages associated with terrorism stemming from a duty to prevent or mitigate acts of terrorism.

Even in the absence of harm, lawsuits have been filed. In September 2004, two tenants of the Empire State Building filed a security-related lawsuit against the building's operators

---

[32] According to Steven Horwitz, "Private-sector firms operate in an institutional environment of profit and loss, which provides an external discipline that ensures they stay focused on their specific purpose." In the case of Hurricane Katrina response, as part of its regular operations, Wal-Mart maintains an emergency command center run by Jason Jackson, Wal-Mart's Director of Business Continuity. The center is usually staffed by six to ten employees who respond to incidents at various stores, although during catastrophes like Hurricane Katrina, the center can include upwards of as many as 60 employees. By being prepared in advance of disasters, Wal-Mart is not only capable of responding quickly in a charitable manner to the needs of disaster stricken citizens in cases of widespread disasters, but it ensures business continuity by quickly reopening stores closed by disasters. In the instance of Hurricane Katrina, "A closer look at Wal-Mart shows that, at the peak of the storm, 126 stores and two distribution centers were closed. Of these closed stores, 'more than half ended up losing power, some were flooded, and 89…reported damage.' By 10 days after landfall, a mere 15 stores remained closed, those that had suffered flooding or severe structural damage." See Steven Horwitz, "Making Hurricane Response More Effective: Lessons from the Private Sector and the Coast Guard during Katrina" (2008) 17 Mercatus Policy Comment 1 at 2 and 4.

[33] Jay N. Rosenblatt, "Unconcerned and Unprepared—A Costly Legal Gamble" (2006) 2 Frontline Security 26.

[34] Order and Opinion Denying Defendants' Motion to Dismiss at 38, *In Re September 11 Litigation*, S.D.N.Y. (No. 21 MC 97).

citing poor security practices.[35] The lawsuit claimed that, "the intentional, reckless, knowing and negligent conduct of [the Empire State Building's operators] poses a clear and present danger and substantial risk of grievous bodily harm and death to persons lawfully on the premises of the Empire State Building."[36] This case, based on negligent security law, a subset of premises liability law, "is premised on the principle that crime is preventable, and that the law places a duty of care upon the party in the best position to take security measures to prevent foreseeable crimes—the property owner or possessor."[37]

Undoubtedly, September 11, 2001, has had a significant effect on the standard of care. Since the standard of care in tort law is measured in part by "proximity" and "similarity," the standard of care for all CEI owners/operators became increasingly strict as CEI owners/operators adopted new security measures after 9/11. As such, CEI owners/operators who do not implement increased security measures risk being seen as operating below the new post-9/11 standard of care.

At the same time, as the events of 9/11 recede further into the past, CEI owners/operators may scale back security measures introduced in the wake of 9/11. This may create legal concerns as a Court may find that the initial security measures adopted post 9/11 set the standard of care, and that the abandonment of these initial security measures means that the CEI owner/operator falls below the standard of care originally set by the CEI owner/operator itself.

Moreover, even if the initial security measures adopted post 9/11 were in response to that terrorist tragedy, many of these measures may have very little to do with preventing the rather extraordinary acts that occurred on September 11, 2001. Some of the measures adopted such as access control passes may be more effective at preventing more common risks associated with unauthorized entry by intruders intent on committing acts of assault, etc. Consequently, for example, an employee of a CEI may bring a legal action alleging that an assault on work premises was a result of a lax owner/operator negligent in meeting the required standard of care.

In this scenario, the plaintiff could compare the level of security at comparable CEI's and find that other CEI owners/operators had hired security guards since 9/11. The result is that prior to 9/11, not having a security guard may have met the standard of care, but after 9/11, deciding not to hire a security guard may subject the CEI owner/operator to legal liability, even though hiring a security guard would do little to prevent or protect against 9/11 type terrorist attacks.

---

[35] Susan Saulny, "Suit Seeks Tighter Security at the Empire State Building" *N.Y. Times* (1 September 2004), B2.

[36] *Ibid*.

[37] Daniel P. Dain & Robert L. Brennan, Jr., "Negligent Security Law in the Commonwealth of Massachusetts in the Post-September 11 Era" (2003-04) 38:1 New. Eng. L. Rev. 73 at 74. The following five paragraphs, with necessary modifications, are based on the logic and argument advanced in this paper.

At the same time, the events of 9/11 brought all types of risk to the forefront of concern and attention. Given all the attention being paid to corporate risk nowadays, it is arguable that even non-terrorist attacks are more foreseeable than they were prior to 9/11. With this greater awareness and more and more CEI owners/operators performing risk assessments, it is becoming increasingly difficult to hide behind the defence of a lack of foreseeability.

As more and more private sector organizations adopt emergency management and response standards, the "foreseeability" of the need to become certified compliant with standard setting bodies will grow. It is, without a doubt, a reasonable expectation that corporations will keep abreast of developments in security protection being adopted by other companies within their industry, and legal liability may flow from such reasonable expectations for those corporations that fail to adopt proven security-related industry practices. As such, the reverse is also true, in that "Maintaining the [industry] standards should then limit the liability of companies and of governments."[38]

Currently, PSC is working with the Canadian Standards Association to develop a new standard that incorporates existing U.S. standards. The Canadian Emergency Management and Business Continuity standard may be based on the U.S. National Fire Protection Association (NFPA) 1600 Standard on Disaster Management, Emergency Management and Business Continuity Programs. According to the Standards Council of Canada, "Endorsed by the U.S. Department of Homeland Security (DHS) and many key U.S. emergency organizations, the National Commission on Terrorist Attacks Upon the United States (9/11 Commission) has recommended that NFPA 1600 be accepted as the common framework standard for private sector national emergency preparedness."[39] This developing Canadian Emergency Management and Business Continuity standard, which will eventually be adopted in Canada by the Canadian Standards Association, in addition to the CAN/CSA Z731-03 standard outlined above, provide convenient standards of care for courts looking to hold private sector CEI owners and operators liable.

In seeking to avoid litigation, the major defence available to public and private sector entities is due diligence. This means simply doing what the "reasonable person" would do in similar circumstances and doing it for all the necessary stakeholders. Among other things, due diligence concerns good corporate governance, best practices, and meeting (or exceeding) industry standards.

However, lawsuits are not the sole avenue leading to national security and emergency management related liability for CEI owners and operators. Legislation establishes national security and emergency management responsibilities for increasing numbers of CEI owners/operators. Most energy companies have little control over their business because of a long history of government regulation. With respect to the nuclear industry for example, the federal government has the power to protect nuclear CEI through an existing regulatory agency such as the CNSC.

---

[38] Richard Cohen, "Public-Private Collaboration: Government can't do it alone" (2006) 1:1 Frontline Security, online at <http://www.frontline-canada.com/FrontLineSecurity/pdfs/06_SEC1_Cohen.pdf>.
[39] Standards Council of Canada, "On High Alert and Prepared for Anything" (2005) 32 Consensus 9 at 10.

The federal *Nuclear Liability Act* establishes the duty and liability of operators of nuclear installations. This legislation establishes the absolute liability of the operator (a CNSC licensee to operate a nuclear installation) to prevent a radiation incident, the capping of that liability exposure (currently set at $75 million), and a process for administering claims against the operator. The *Nuclear Liability Act* also bars claims against others for alleged breaches of the operator's duty, and provides that the operator has no right of recourse or indemnity against others for breach of this duty.

Recently, the federal government introduced Bill C-5, *An Act respecting civil liability and compensation for damage in case of a nuclear incident*, which if passed into law, will repeal the *Nuclear Liability Act*. Bill C-5 restates the key principles of the liability regime established under the *Nuclear Liability Act* for damage caused by the occurrence of a nuclear incident in Canada, namely, that:

- The operator's liability is exclusive; that is, no person other than an operator is liable for damage caused within Canada; and
- The operator's liability is an absolute, strict liability requiring no proof of fault or negligence

In addition, there are a number of important changes introduced by Bill C-5, the most important being a significant increase in the maximum liability for operators from $75 million to $650 million.

It should also be noted that with respect to the electricity sector in Canada, enforcement of North American reliability standards establish mandatory obligations on public and private sector companies and organizations with associated penalties for non-compliance.[40] The North American Electric Reliability Corporation (NERC) oversees eight regional reliability entities and encompasses all of the interconnected power systems of the contiguous United States, Canada, and a portion of Baja California in Mexico. NERC's major responsibilities include developing standards for power system operation and monitoring and enforcing compliance with those standards. NERC's Reliability Standards are currently mandatory and enforceable in Ontario and New Brunswick.[41]

In Ontario, for example, on April 4, 2006, NERC submitted applications for recognition to the Ontario Energy Board, the National Energy Board, and the other provincial regulators. The Ontario Ministry of Energy responded on November 28, 2006, by officially recognizing NERC as the Electric Reliability Organization (ERO). Ontario's Independent Electricity System Operator's (IESO) Market Assessment and Compliance

[40] Similar mechanisms exist for other energy sectors, including oil and natural gas producers and pipeline operators.

[41] NERC is working to make their Reliability Standards mandatory and enforceable with the remaining provinces, in addition to seeking recognition as the Electric Reliability Organization with the remaining provinces. See Independent Electricity System Operator (IESO), "Electric Reliability Organization (ERO): Impact on Ontario" (2007) 22 Quick Takes 1 at 2.

Division conducts the compliance process by establishing and enforcing standards and criteria for electricity reliability purposes. This means that NERC and the Northeast Power Coordinating Council (to which Ontario, Quebec, and the Maritime Provinces belong) reliability requirements are adopted in the market rules along with other Ontario-specific reliability standards that the Ontario IESO implements.[42] As such, enforcement of North American reliability standards create national security related responsibilities for a number of CEI owners and operators.

V. CONCLUSION

In summation, there is an inevitable legal imperative on the part of both government and private enterprise to protect CEI. Inadequate counter-terrorism practices by government may be deemed to be negligent in a post 9/11 world, and neglect by government of its emergency management related responsibilities by taking actions that harm the public, may lead to claims being sustained against it by a finding of a neglected duty of care. Likewise, if a government or agency of government fails to take action to aid in the security of citizens in preventing or minimizing cascading damages from a terrorist attack on CEI, and preventing harm upon citizens and/or industry, claims may be sustained by a finding of negligence.

In addition, if a government or government agency fails to pursue public-private partnerships or the "manner and quality" of such partnerships fail to rise to an adequate level of standard of care, or public sector entities fail to gather, evaluate and/or disseminate critical information in regards to the protection of CEI, then tort law claims may be sustained against the government. Private sector owners and operators of CEI must also consider their vulnerabilities and where necessary, should address them appropriately with government.

Furthermore, in the event of a security breach, terrorism related or not, tort liability would likely ensue against private sector owners/operators of CEI if investments in security were not made that might have reasonably prevented or mitigated any damages. Likewise, those private sector CEI owners/operators put on notice by government through governmental national security related strategies, would have a legal imperative to work cooperatively in partnership to secure CEI. Those CEI owner/operators unable to adequately secure their facilities may also have a duty to seek government assistance in partnership or risk legal liability. Government policy and strategies, industry and association emergency management and business continuity standards, and other regulatory standards provide convenient standards of care, and as such, are attractive tools for courts to use in navigating through these increasingly important issues and in resolving national security and emergency management-based litigation.

Although what is reasonable today is understandably well beyond that which existed prior to the terrorist events of 9/11, ultimately knowing exactly what legal liabilities would result from harm caused to citizens and industry from a failure by public and private sector owners and operators to aid in the security of CEI, is for the time being,

[42] *Ibid*. at 3.

based more on enlightened supposition than hard legal fact. Nevertheless, because so much of the security and prosperity of Canadians rests on CEI, "governments and the private sector should feel obligated to do what they can to reduce risks by increasing their efforts to work much more closely together in protecting the public and securing the economy."[43]

[43] Jacques J.M. Shore, "Cooperation a Legal Imperative?" (2005) 6 Frontline Defence 13, online at <http://www.frontline-canada.com/Defence/pdfs/05_6_Shore.pdf>.