

Public-Private Collaboration Government can't do it alone

By Richard Cohen

FrontLine Security, vol.1 no.1

After 9/11, governments around the globe sprang to respond to the new threat. In Canada, the federal government implemented major structural changes and allocated billions of dollars to strengthen National Security and Public Safety. As well, recent natural catastrophes and public health scares have reminded us that terrorism is not the only danger we face. Although most governments have reacted energetically to these new challenges, the rest of society, including the business community, have for the most part, been sitting on the sidelines.



In an era in which war and catastrophe now comes to us instead of us to them, business, non-governmental organizations and individual citizens must all take an active part in national security. In Canada, private companies own and operate a very large portion of the critical infrastructure that provides our banking, our energy, our communications, our food and our water. Thus, the people who run these companies have a heavy responsibility for the security of our economy and our society. But governments must help them share this burden.

No one part of our infrastructure can function on its own for long. A dense web of interdependencies has evolved as our economy has become both more efficient and more complex. Take the food supply chain for example. It can be disrupted by a power blackout that shuts down refrigeration systems and computerized cash registers in supermarkets. Damage to a major oil refinery or pipeline can affect fuel supplies for vehicles deliver food to the retailer. A pandemic can put the people who run the food supply chain in bed, in hospital or at home looking after sick family members. A cyber attack can shut down the banking system and disable credit cards and cash machines leaving people unable to purchase the food.

In short, virtually everything is now dependent on everything else and much of the onus for maintaining this vast web of interdependencies falls upon the private sector. In a large scale emergency, governments, on their own, have no hope of providing safety and security to the citizens they were elected to protect.

How then can government work with the private sector to make our society less vulnerable? I suggest the following key guidelines for strengthening public-private sector collaboration:

Effectively Communicate Risk. Governments must be open and honest with the public in assessing risk. Worries about security of information, privacy, alarming the public and admitting that they can't protect all the people all the time does make the job difficult. And yet experience in countries like Britain and Israel, long subject to terrorist attacks, shows that people are more robust and ready to accept risk than their leaders often assume. Discussing risks and threats with industry should be easier than communicating with the general public, but even here the process has a long way to go. The problem works both ways; governments are traditionally loath to share sensitive information with 'outsiders' and businesses are reluctant to reveal their vulnerabilities to government and competitors. Both sides must build trust and overcome these suspicions.

Share Information. Governments and agencies, such as CSIS and the RCMP, must be more willing to share information with 'first responders' who are expected to react to attacks or natural disasters. Security of sensitive information must be respected but the federal government has been very slow to develop ways of clearing key persons outside government to receive the information they need. Private sector companies must also have enough information to make sensible risk assessments on which to base their planning and allocate their resources. They need a degree of confidence in deciding on: 'How much is enough?' and 'Are we unnecessarily spending more on security than our competitors?'

Develop Openness and Trust. Industry must be more forthcoming with government and with their suppliers, competitors and customers about their security challenges. Total openness is probably not realistic but companies can exchange ideas on common problems and best practices. Although some industry associations have made good progress in this area, information sharing within or across sectors, or with governments is not satisfactory. In the US, the process is arguably better developed. But even there it is far from complete. Informal "ISACs" (Information Sharing and Analysis Centers), have been established, often with government funding, within sectors including banking and finance, surface transportation, cyber and information technology, electricity, public health, gas and oil, etc. The ISACs exchange information among members and develop and share best practices to improve resilience and sustainability in times of emergency. However, because of the fear of government acquiring sensitive inside information, the Department of Homeland Security is largely excluded from the ISAC processes. In Canada, as well, industry is very concerned about the confidentiality of its proprietary information. An important step for government would be to amend the Access to Information Act to assure the private sector that any sensitive commercial information it receives can be properly safeguarded.

Provide Clear Governance Structures. A well-understood and practised governance system for emergencies is still not in place within the federal government or between the federal, provincial and municipal governments. Each jurisdiction believes it understands its own mandate but there is a lack of coordinated planning for emergency scenarios. For this reason, companies are not confident that they understand the governance framework in which they will operate during an emergency. This uncertainty about who should be doing what and when, led to confusion and delays before, during and after Hurricane

Katrina. The US government was ridiculed for its failures in the wake of Katrina, but Canadians should not be complacent that we would necessarily do better in such a large scale emergency. Ambiguities must be eliminated. This will take a lot of negotiation and compromise – and the time to start is now.

Work Toward Interoperability Standards. There is still a lack of interoperability in communications systems, data sharing and key equipment between federal agencies and between the federal, provincial and municipal governments. For this reason, large-scale operations in response to emergencies like radiological, biological or chemical attacks or natural disasters will be difficult and largely ad hoc. Aside from the RCMP, which has country-wide common systems, most Canadian police forces can't communicate or easily share data with each other. Integrating reinforcements from other cities or provinces could prove slow and difficult. The federal government has been working on commonality issues but remains a long way from achieving true interoperability, even between government departments, let alone provinces, cities or the private sector. The federal government must take the lead in setting parameters and guidelines, and must ensure implementation by all levels of government and the private sector. Of course, industry wants guidelines not more regulations. It prefers voluntary standards but ultimately those standards must be correctly set and implemented.

Encourage Joint Research and Development. Keeping ahead of the terrorist with innovative technology is one of the keys to preventing and mitigating attacks. Clever technology can also help alleviate the worst effects of natural disasters. The Chemical, Biological, Radiological and Nuclear (CBRN) Research and Technology Initiative (CRTI), run on behalf of the federal government by Defence Research and Development Canada, is a model for public-private cooperation in this area. CRTI-funded projects are conducted jointly by government laboratories, private companies and universities. The program promotes the development of technology and standards for police forces, fire departments, medical teams and other first responders to CBRN attacks. The CRTI is a real success story but it's limited to a relatively small number of projects each year. The government could use the CRTI model to expand and broaden collaboration across the full spectrum of the national security and public safety sector.

Reduce Legal Liability by Setting Agreed Standards. Liability for damages and harm to customers and persons affected by real or perceived security failures has become a major concern for both business and government. The former operators of the World Trade Center are currently the target of huge class action law suits that allege all kinds of security lapses prior to and on September 11th. Governments may also be legally liable if they can be shown to have fallen short in their planning, training or execution of emergency plans. In this area, government must take the lead to work with industry in developing standards of security and safety. Maintaining the standards should then limit the liability of companies and of governments. This arrangement should be codified in legislation and such laws would help persuade private companies that good security makes good business sense.

Practise, Practise, Practise. As the saying goes, an emergency is no time to be exchanging business cards. People at emergency measures organizations and in every other government department and agency with a role in emergency management must know one another long before a crisis arrives. Private sector operators of critical infrastructure and other sensitive businesses and industries must develop close relations with their government, police and other collaborators. The best vehicle for preparing for the worst is to plan and train together in realistic scenario-based exercises on a regular basis. This requires a real change of culture and here again governments must lead. Exercises can never fully simulate real situations. But they can identify weaknesses in governance structures, command and control, communications, interoperability, passage of information and gaps in procedures, plans and training. Properly run and frankly and openly debriefed, exercises develop confidence, trust and personal links between people who will have to work together in a real emergency.

Governments at all levels in Canada now recognize that protecting Canadians and the Canadian economy is not a job they can do alone. Since September 11th, considerable time, effort and money have gone into developing better understanding and collaboration between the public and private sectors. At the national level, Public Safety and Emergency Preparedness Canada, Transport Canada, Health Canada, Natural Resources Canada and the Department of National Defence are at the forefront of these efforts. Many industry associations and companies across the country also play an active role. So are non-governmental organizations like the Red Cross and the Conference Board of Canada which is promoting public-private sector dialogue and joint research through its conferences and its newly formed Centre for National Security.

We are still at the beginning of a long and complex process. Implementing these guidelines will require resources, dedication and good will from all sides over a long period of time. But, in the new and dangerous world we live in, the safety of Canadians and our economy is well worth the effort.

-30-

Richard Cohen is President of RSC Strategic Connections. He has advised countries in Central and Eastern Europe, the Balkans and the former Soviet Union on developing national security policies. He has lectured widely and published numerous articles on national and international security matters. He is working with the Conference Board of Canada to promote government-industry collaboration on national security and public safety issues