

Smart Security Needs Coordinated Solutions

On 11 September 2001, the world was transformed by 19 airline hijackers. Among many other effects, the sudden arrival of international terrorism on our doorstep stimulated a burgeoning new industrial dimension; homeland security and public safety technology.

Within hours of the 9/11 attacks the call went out across the United States, and most of the rest of the world, to tighten security. Airports, and airlines in particular, searched for holes in their screening systems which the 9/11 terrorists apparently penetrated easily and undetected. Human error and regulatory failure seemed clearly to blame, but so was the relatively unsophisticated technology in place on the day.

An Industry Takes Off

After 9/11, the sudden explosion in demand for public safety technology of all kinds was no short term phenomenon. A new industry was created, and it is here to stay. A series of man-made and natural disasters, occurring with apparently increasing frequency and intensity have subsequently made the long term need very clear. Technology, designed to protect people, infrastructure and the economy, has become part of our lives for years to come.

In the wake of the attacks on New York and Washington, the U.S. Congress allocated billions to homeland security. Much of it went to new technologies to improve security at airports, seaports and borders. In late 2001, the Canadian government announced an \$8 billion program over five years for a major overhaul of our national security and public safety apparatus. In December 2003, the department of Public Safety and Emergency Preparedness was created. In Canada, as well as in

many other parts of the world, the public safety 'industry' was solidly launched.

Today National Security and Public Safety Technology is a growing business. In several ways it parallels the defence industry, and traditional defence firms were quick to identify the new needs and the opportunities in the aftermath of 9/11. A myriad of non-defence related companies, from manufacturers of cameras and detection and surveillance equipment to providers of computers, communications and software also became very active in security and safety. It seems clear that while traditional defence spending will probably remain relatively flat, budgets for unconventional security technology will continue to grow.

Resources Well Spent?

Perhaps the biggest challenge is to adapt our thinking to the new reality.

Everything happened so fast after 9/11 that much of the huge increases in homeland security and public safety budgets, on both sides of the border, disappeared into massive government reorganizations.

Vast amounts of effort and resources were sucked into the creation of the Department of Homeland Security in the US and Public Safety and Emergency Preparedness Canada. And there was a rush to put technology into airport security and the protection of other potential terrorist targets. In Canada, for example, \$1 billion was spent in a 5-year program to install Explosive Detection Systems for airline passenger baggage screening at virtually all Canadian airports. However, money was not always spent wisely. In some cases, off-the-shelf equipment was bought quickly to fill security gaps before a detailed requirements study was made.

And there was often little coordination or regard to interoperability with technologies in use by other agencies for similar purposes.

In April 2004, Canada's first *National Security Policy (NSP)* included another \$690 million for public safety. A year later, the *NSP Progress Report* announced a further \$1 billion (over five years) for national security and public safety, including over \$400 million for border services and for maritime transport security – a good proportion of which will be devoted to the acquisition of new technology.

Not surprisingly, weak coordination of diverse requirements and procurement characterized the rush to buy the new equipment, sometimes within the same government department or agency.

Results often fell short of expectations. Consequently, interoperability between federal government agencies and other levels of government and law enforcement suffered. For example, city and provincial police forces cannot easily communicate with the RCMP or with each other. This was one of the major problems U.S. agencies had in dealing with the aftermath of hurricane *Katrina*. Interoperability of voice communications, data transfer and other less-obvious but important technologies is still distant.

After almost five years, and near the end of the first cycle of technology deployment, we need to look at more coordinated solutions to organizational and technological issues.

The Users

The public safety user needs are vastly different from the traditionally well-defined defence community, which are limited and well-known. In contrast, the public safety community covers an almost infinite range of government departments and agencies, stretching well into the private sector. It ranges from governments to owners and operators of critical infrastructure, sensitive industries, public transport, shopping malls, concert halls, cinemas, sports arenas and many others.

In Canada, public safety technology users fall into three groups:

- the federal government and its agencies
- provincial and municipal governments and first responders
- the private sector, including critical infrastructure and other sensitive industries and businesses

In the first group, the major users are: the RCMP, CSIS, the Canadian Border

Services Agency (CBSA), now all under the umbrella of Public Safety and Emergency Preparedness Canada (PSEPC); DND and the Communications Security Establishment (CSE); Transport Canada and the Canadian Air Transport Security Agency (CATSA); the Public Health Agency, under Health Canada; and the Canadian Coast Guard, a part of the Department of Fisheries and Oceans. Billions in extra security dollars have flowed to these federal agencies.

Very little federal money has yet found its way to the second group, the provinces and the 'first responders' who argue that they need it most. Some provinces and municipalities have done much better than others in drawing up emergency plans and equipping themselves to meet a variety of threats, however, there has been little coordination between them to date.

The third group, the private sector, has been left largely on its own. The federal government has given little encouragement to private business to invest in their own security. Except for the most sensitive industries, like nuclear power, banks and telecommunications companies, progress has been slow. Success in the private sector has been largely independent of government.

Recently, PSEPC, Transport Canada and several other government departments have begun to develop nationwide strategies for critical infrastructure protection and transportation security. In the meantime, most potential targets in Canada remain soft and vulnerable.

New and emerging technologies can make a difference. The challenge is that industry providers and users have yet to come to terms with how best to define their requirements, to set standards of performance and interoperability, to encourage R&D, and to coordinate procurement and deployment.

The Next Challenge

Gradually, weaknesses in the air transportation security system are being fixed. And a start has been made in plugging some of the holes in ports, sea transport and cross-border security. However, as it becomes harder for terrorists to penetrate defences in one area, they will look for other vulnerabilities.

Surface transport, including mass transit systems in big cities, is much more difficult to protect than airports, seaports

and borders, especially from an internal enemy, as the Madrid and London attacks demonstrated. Terrorists pass new lessons and tactics quickly around the world and Iraq has shown that anywhere large numbers of people gather is a potential target for those intent on causing as much mayhem as possible. The number of these targets here at home is infinite.

Iraq has also shown us that any piece of vital infrastructure is also at risk, from pipelines to electricity stations and fuel storage depots. In Canada and the U.S., most of these facilities are owned and operated by the private sector, but too little attention has been paid to how govern-

ments and business can help protect each other. Public-private sector collaboration is essential, but despite the efforts of government, industry associations and organizations like the Conference Board of Canada, it is still in its infancy. Clearly there is a lot of work left to be done. ■

Richard Cohen is president of RSC Strategic Connections, based in Ottawa. He has wide international military and academic experience, and practical expertise in counter-terrorism and national security policy development. He is currently organizing activities for public-private sector collaboration on national security for the Conference Board of Canada.

PLEXSYS
 International Canada, Inc.

Team Up With An Original!

- Proven-capability ASCOT V Radar Simulator
- Tactical Radar Control Expertise
- NORAD Aerospace Control Expertise
- AWACS Mission Crew Control Expertise
- Distributed Mission Operations (DMO)

Meet PLEXSYS International Canada at the upcoming tradeshow and see why people want us on their team from day one.

PLEXSYS - An Original DMO Partner

I/TSEC 2005 Booth #571

1238 Barrwell Cr. Ottawa, Ontario Canada K4B 1K4 www.plexsysipi.com 613.835.7539

• PUBLIC SAFETY • NATIONAL SECURITY • EMERGENCY RESPONSE •

To apply for a free trial subscription, visit:
www.frontline-canada.com

FRONTLINE Security

Are you a FEDERAL GOVERNMENT LEADER in national security or public health and safety? Are you a PROVINCIAL or MUNICIPAL DECISION-MAKER responsible for implementing public safety and emergency response measures? Are you a FIRST RESPONDER ready to come to the rescue during emergencies? Are you an INDUSTRY OFFICIAL providing equipment & services to these important sectors?

FRONTLINE SECURITY is Canada's only crisis management magazine. A nationally-distributed publication, it provides a valuable forum for these critical sectors in a glossy magazine format. Editorial contributions from influential leaders and experienced experts cover issues faced by the departments, agencies and industries responsible for Canada's safety and security challenges. *Launch date: 2006*