DRDC Suffield photo

Live Agent Training: Decontaminating suspect luggage in an 'airport' scenario.

SCIENCE AND TECHNOLOGY: A KEY COMPONENT OF COUNTER-TERRORISM STRATEGY

by Dr. L.J. Leggat

The terrorist attacks in the United States in September 2001 changed forever our perspectives on national defence and security. The impact on North America has been particularly evident from a Canadian perspective; however, the reaction from all regions of the globe is clearly evident. Terrorism of course has been a threat for many years, but in the case of the 2001 attacks in the United States two factors seem to differentiate them from previous acts of terrorism.

The first factor is the sophistication and magnitude of the attacks. Clearly the planning for the operation spanned many years and involved many people in several countries. Considerable effort went into training for, and planning and synchronizing the activity. The impact was horrible, but if all aspects of the plan had been executed, it would have been worse.

The second factor is the size and power of the Al Qaeda network, which is an operation of global scale intent on developing armies of revolutionaries and terrorists armed with the most deadly of weapons.

Shortly after the September 2001 attacks, the President of the United States stated that defeating these forces would not be a short-term proposition. I believe that today we understand the accuracy of that statement more than we did at the time.

If there is one thing that 11 September forced us all to do, it was to develop a clear understanding of the vulnerabilities that our societies have developed as a result of the great freedoms that we all enjoy in our democratic states. The freedom and liberty that permit the movement of people and goods, that ensures individual rights and that promotes intense confidence and optimism come with certain vulnerabilities and weaknesses, with which democracies have always had to contend. These freedoms have led to great prosperity, and relinquishing them would necessarily have a startling impact on global well-being. So the dilemma is: How do we strengthen our defence and security posture without endangering the liberties which we have gained over centuries of hard work?

The answer is not simple. Many governments, including Canada's, have been developing responses to this question since 11 September. The response tends to be multi-dimensional, involves many departments and agencies, and engages players who do not normally work together, at least not under such conditions. In its simplest form, departments and agencies are working together to develop greater understanding of the risks and greater ability to anticipate, prevent and respond. Emphasis appears to be focusing on where capability is inadequate and where improvements need to be made. This process necessarily relies heavily on risk management techniques. Solutions by definition will not be discrete or closed form. Indeed probabilities will always play a significant part and the robustness of solutions can only be verified through extensive testing against scenarios using modeling and exercise methods.

Dr. L.J. Leggat *is Assistant Deputy Minister Science and Technology in the Department of National Defence.*

Because the terrorist threat we face is transnational, the response must have dominant international dimensions. Challenges that we face internally in the development of organizational and procedural approaches will be magnified many times when international coordination comes into play.

There are many opportunities to use science and technology (S&T) to address the needs and I will discuss these later. Some say that S&T is the key to ensuring lasting freedom while dealing with the vulnerabilities that others would exploit. At the outset, S&T will bring together some unwilling partners who will with time become the closest of associates. Knowledge, and how we manage it, is a key enabling factor. The S&T associated with knowledge management will thus be important, in particular that S&T which enables new ways to correlate seemingly unrelated pieces of knowledge and information.

DRDC Suffield photo

Live Agent Training: Sampling for chemical warfare agents in a mock terrorist laboratory.

ORGANIZATION IN A STATE OF FLUX

An early and obvious impact of the terrorist attacks has been a massive examination of a nation's organizational structure for preparedness, prevention and response. In the United States, for example, we have seen the formation of the Department of Homeland Security. In Canada, a special committee of Cabinet called the Public Security and Anti-Terrorism Committee coordinates government investment and organization around the issue. The terrorist threat has not spawned any new federal government departments in Canada. It has, however, significantly increased the importance of certain interdepartmental processes, and a new sense of urgency is present. Before 11 September, the Canadian government had created the Office for Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) to provide government leadership on the full range of emergency management activities, as well as to provide national leadership in emerging areas of critical infrastructure protection including both the physical and cyber dimensions. With the terrorist threat and the concern about the use of chemical, biological or radiological/nuclear (CBRN) weapons, OCIPEP's mandate includes coordinating the development of CBRN response capability nationwide.

Canada invested $280 million in immediate measures (such as enhanced policing, security and intelligence) in the wake of the attacks in the United States. The five-year $7.7 billion investment announced by the Canadian government in December 2001 allocated resources to a number of areas. Air security has been strengthened by the creation of an Air Security Authority and by utilizing air marshals, better screening and enhanced policing. National security posture improvements will be brought about through increased investment in intelligence, policing, emergency preparedness and military deployment. Finally we are working closely with the US on co-managing the border. This includes acquiring new screening technology, developing integrated enforcement teams and better information sharing procedures, and installing improved infrastructure at the border. These new investments will drive new organizational groupings. The investments will also create new needs among those responsible for defence and national security; many of these needs can only be addressed properly through the application of S&T to the delivery of solutions.

Those who work in and deliver S&T must be ever conscious of changes to the organizational structure, because this structure determines the ultimate customer for S&T products. The organizational flux that we are experiencing is changing traditional customer communities and is affecting well-established links between research centres and their customers. If S&T organizations are to remain relevant to the needs of the nation, they must stay abreast of organizational shifts and develop relationships, perhaps with entirely new customer communities.

This is particularly true for defence research where the relationship between defence laboratories and the military customer has been very close in most nations. As the line between defence and national security becomes blurred, defence labs must seek a broader client base to ensure that they remain relevant to national interests and that their expertise is widely available to all agencies and departments whose mandates involve security and national defence.

Generally speaking, however, national security departments and agencies do not have strong science capacities, except in narrow applications such as forensics. Furthermore, at least in Canada, there is no culture or history of cooperation between the general science community and the security community. Clearly this presents new challenges for those of us in government who are responsible for activities as diverse as fire-fighting, policing and hospital care, and the defence of the nation. The centre of gravity for our adversaries is the very freedom we have striven to win and maintain. The front is no longer in some distant land, nor even at our borders – it is within. This reality is changing how we organize our defence and national security assets. Defence science must change too.

DEVELOPING FLEXIBLE APPROACHES

A flexible approach to countering terrorism starts with sound and well-tested response plans, which set out the roles and responsibilities of agencies engaged in the war on terrorism. In many countries such plans have been in existence for some time.

"Knowledge, and how we manage it, is a key enabling factor."

Canada has been tested by a variety of emergencies in recent years, such as the Manitoba floods, the Eastern Canada ice storm, the Saguenay floods, numerous tornadoes and the threat of foot-and-mouth disease. Our response system has worked well. In the cases of the Manitoba floods and the ice storm, the Canadian Forces were called to the Aid of the Civil Power for extended periods of time. All levels of government are familiar with and have considerable training and experience with the response mechanisms in these situations.

The level of government closest to the emergency responds first, with higher levels being brought in as required. A National Support Plan, managed by OCIPEP, specifies how federal expertise and assistance can be brought to bear. Specific plans address specific emergencies. For example, we have an Earthquake Response Plan, a Nuclear Emergency Response Plan and a Space Objects Re-entering the Atmosphere Plan. For their part, cities, municipalities, provinces and territories all have emergency management organizations and emergency response plans for their jurisdictions.

Few of these well-established and well-tested plans anticipated terrorism as the cause of an emergency. For example, Agriculture Canada and the Food Inspection Agency did not have emergency response plans that anticipated the possibility of diseases being deliberately and maliciously introduced into the food system, herds or farms.

Canada's National Counter-Terrorism Plan (NCTP) is the responsibility of the Solicitor General of Canada. We have little experience in working with this plan or in dealing with terrorism in Canada. The most recent events, the Air India and Narita Airport bombings in 1985 and the Ressam Affair in 1999, had Canadian origins, and in the case of the Air India bombing, it killed Canadians, but did not affect persons or facilities in Canada.

In response to the changed security environment, significant rethinking is underway. The Department of the Solicitor General is leading a review of the NCTP, and OCIPEP is leading a major review of the government's emergency readiness and response capacity. The OCIPEP is also discussing the development of a national framework for emergency readiness and response with the provinces and territories. Rather than working independently, the emergency management and counter-terrorism communities are working collaboratively since they recognize that they face many common planning factors – threats to the safety of individuals and communities, the psycho-social response of citizens and property damage to name a few.

Since 11 September, we have seen a resurgence of interest and participation in exercises such as "Thin Ice" (anthrax in Vancouver) and "Dark Winter" (smallpox in Salt Lake City). The efficacy and robustness of the plans will also be assessed through a process of mapping channels of information flow and decision-making. Such mapping allows us to understand the interdependencies in the response structure and to know where weaknesses exist in our ability to anticipate, prepare and respond to terrorist events.

Traditional operational research (OR) skills can be used to good advantage in assessing our preparedness to deal with terrorist events. OR specialists are experienced in applying their analytical skills to war gaming and post exercise analysis. Techniques developed for the military are equally applicable to the broader defence and national security scenarios. However, our engagement of the OR community in Canada is very limited and needs to be expanded.

It is evident that providing a flexible organizational response to terrorist threats involves the creating of a network of those associated with prevention and response. A network of individuals in operations must be able to adapt to the nature of an emergency. Its leadership would be expected to change depending on the emergency or suspected emergency, and the phase of the operation (i.e., preparation, prevention, response, etc.). The rules by which agencies work together, be they municipal, provincial in the case of Canada, or federal, need to be clearly defined in the response plan framework, and ideally such networks would function quickly and effectively when faced with any type of situation.

The S&T community needs to be linked in a similar manner. While the traditional mandates of our government, university and industrial R&D centres still apply, we need to find new ways of linking S&T intellectual capital and infrastructures within our countries and internationally so that the full S&T capacity available can be brought to bear on the critical operational challenges.

In Canada, we have been working with the concept of clusters of R&D performers made up of federal government, university and industry research centres. These clusters are virtual organizational structures that link labs which have related, relevant capability. The labs do not have to be in the same location; in fact, in most cases they are not. The specific

DRDC Suffield photo

Live Agent Training: Disarming an improvised explosive device.

application of the first cluster concept has been to the CBRN threat through the formation of the CBRN Research and Technology Initiative (CRTI). This programme was established when Budget 2001 was tabled and is designed to contribute to the development of an integrated national capability to deal with CNRN threats and incidents. Within CRTI's organization, we have formed three clusters: chemical, biological and radiological/nuclear. Each cluster has a leader and a charter governing how the cluster operates. In CRTI, the principal cluster members are federal and other government laboratories, typically from the departments of health, environment, natural resources, industry, defence, agriculture and fisheries and oceans. The university and industry participation is engaged through the specific R&D projects undertaken within the cluster. The clusters have two principal roles within the CRTI: the first is to provide S&T advice to the response community through links which are being created between the clusters and the operational networks through the National Emergency Response Plans; and the second is to perform R&D to advance technology in certain key investment areas that have been defined through a threat assessment and gap analysis process. Linking the clusters to the national response framework is particularly important as it is the only this federal lab network that is capable of providing rapid and accurate scientific assessment of the nature of a CBRN incident.

Investment Priority	Bio	Chem	RN
Cluster Management and Operations			
C4I for CBRN Planning and Response	1	1	2
R& D for Training and Equipping 1st Responders	5	3	4
Prevention, Surveillance, and Alert	1		2
Immediate and Near Term Consequence Management			1
Criminal Investigation Capabilities			
S&T Dimensions of Risk Assessment	1		
Public Confidence and Psycho-Social Factors			

Figure 1: CRTI Investment Priorities showing where approved projects impact.

We are also developing a similar cluster concept for information security. Here, federal labs from the defence and industry departments are linking research objectives and teams to generate technology to address both civil and military requirements for network security. While the applications differ somewhat, the underlying tools and methods have sufficient commonality to be of considerable use in both military and civil environments.

One final organizational note in S&T's role in combating terrorism pertains to the development of threat assessments. Risk assessments, which are the underpinning of an analysis of the threat, rely heavily on scientific judgments concerning the feasibility and difficulty associated with adversaries engaging specific scenarios. Linking the S&T community to the broad security and intelligence framework within a country is essential to the success of counter-terrorism actions. An accurate threat assessment founded on solid scientific judgment will help ensure that scarce resources are invested in the best possible way towards strengthening defence and national security capability.

THE ROLE OF S&T

In Canada, the S&T dimensions of national security and counter-terrorism were examined in some detail during the spring and summer of 2001. When the attacks occurred in the United States, we were well advanced in our thinking about what kind of new programmes would be needed to contribute to enhanced national security. The work was carried out within an interdepartmental group that was looking, at the time, at a number of cross-cutting or horizontal issues before government and developing means for the R&D community to work together around each specific issue. A programme called the Federal Innovation Networks of Excellence (or FINE) was proposed for creating networks of federal, university and industry S&T performers to address issues of national importance. As it turned out CRTI became the pilot project under the FINE model.

The National Security and Counter-Terrorism theme engages five specific areas of R&D endeavours: chemical, biological, radiological and nuclear protection; disaster consequence management; information infrastructure security; physical infrastructure security; and knowledge management of surveillance and intelligence information.

Of these five areas, the CBRN is currently the most highly developed because of the federal government's $170 million investment in the CRTI. To date 24 projects have been funded in nine investment areas, as shown in Figure 1.

The programme has engaged 10 federal departments and agencies, 11 industries, and 10 universities in these 24 projects. Funding of another 20 to 25 projects commenced on 1 April 2003, with about that number of projects coming on line every year for the next four years at a minimum. In the first round of funding the investment has been primarily in the areas of R&D for training and equipping first responders and in immediate and near term consequence management. The projects address both the immediate opportunities brought about by accelerating technology that is already in its final stages of development, and the longer term R&D needed to bring forward solutions to the tough technical problems that need to be addressed in many of the investment areas.

Another area, which is also developing well, is information infrastructure security. Here a solid network has been established among the principal operational authorities, OCIPEP and the Communications Security Establishment (CSE), and the R&D community comprised of Defence

"Traditional operational research skills can be used to good advantage is assessing our preparedness to deal with terrorist events."

"Getting the dynamic right between those who are concerned with the operational aspects of counter-terrorism and those who deliver the S&T advice and products is a critical piece in the development of the national response framework."

Research and Development Canada (DRDC), the Communications Research Centre and CSE's research department. By examining the evolving threat and assessing both military and civil vulnerabilities, the parties have identified four principal areas for collaborative activity: intrusion detection tools and methods; security of Government of Canada systems; development of IT security standards and best practices; and cyber incident response tools and techniques. Other areas of interest that are being addressed by DRDC include protection and integrity of networks; multi-level security in coalition operations; recovery from system attacks or failures; and warning against high power microwave and non-nuclear electro-magnetic pulse attacks.

Although the other areas of R&D are less developed, it is still worth discussing the opportunities in each. In the case of disaster consequence management we see two principal areas of need: R&D to develop techniques and technologies to treat mass casualties, and advances in biosensor imaging, information processing, miniaturization and biotechnology (which could lead to real time monitoring of health status indicators), automated treatment deliverance, field tolerant diagnostic devices and triage aids for trauma and other injuries.

Canada's physical and information infrastructure includes oil and gas production and distribution infrastructure, electrical power generators and grids, communication and transportation networks, banking and government services, and the water supply and food chain. The array of R&D possibilities here are enormous, and this in itself presents a significant challenge. Clearly understanding vulnerabilities and the relationship among the various types of physical infrastructure is an important first step. For example an attack against one class of infrastructure could have significant ripple effects throughout the others. Exposing vulnerabilities in these systems is relatively straightforward; understanding which vulnerabilities are truly critical might take some significant effort.

It is in this latter area where effects based operations (EBO) might play a useful role. EBO is not a new concept; it allows us "to conceive and plan operations in a systems framework that considers the full range of direct, indirect and cascading effects, which may be achieved with differing degrees of probability by the application of military, diplomatic, psychological and economic instruments."[1] It is used in the planning and execution of military operations; however it has equal potential for use in understanding how others might exploit the vulnerabilities in our infrastructures to achieve their aims. EBO based analysis should allow us to determine critical linkages and cascading routes between classes of infrastructure thereby allowing us to pinpoint and understand our most important vulnerabilities. Modelling all aspects of our infrastructure will be no simple task, and it will not come without considerable investment.

Finally there is the question of our surveillance and intelligence information and the potential that knowledge management techniques offer in ensuring that correct and relevant information is available when and where needed. Here we face a number of problems: too much data (some of which is wrong) and too little information and knowledge. We know how to correlate data, but we are not as good at correlating information and knowledge. We also have problems sharing information nationally and internationally. Security gets in the way of electronic transfer and slows us down. Organizational barriers sometimes make it difficult to share information freely among departments and agencies.

Technology has a role to play here, but the solution goes beyond simply calling on new technology. New procedures and protocols need to be developed for information sharing that make best use of current and evolving Knowledge Management (KM) techniques. The integration of the human into the knowledge management construct is essential. After all it is humans who create knowledge, so to manage it without the human in the loop would be unproductive. Understanding how to do this is the key challenge. The application of KM to the intelligence and surveillance business is rich with opportunity from knowledge creation, capture and acquisition; to organization and dissemination; and sharing, use and learning.

Modern information technologies have important contributions to make. Some promising areas include content management, mapping knowledge, knowledge push and pull, software agents and decision aids, visualization and data mining, portals, web collaboration, and lessons learned. These areas are particularly ready for exploitation; they involve an important marriage between humans and the body of knowledge they have created.

In the debate about S&T and counter-terrorism two central issues arise: capacity and quality. Both are important. Governments need adequate breadth and depth of scientific advice to make sound judgments. The quality of that scientific advice is a function of the people and the organizations to which they belong. Quality science available on an international scale will contribute to good decisions and strong public confidence. Countries the size of Canada cannot do everything in this or any other area. We, therefore, rely on continued strong relations among allies so that we can gain access their technological depth when developing advice on Canadian defence and security.

CONCLUSION

The national response framework to terrorist attacks will vary from nation to nation depending upon government structure and policy. It is also fair to say that the science and technology advice that governments receive on issues ranging from assessment and preparedness to response and consequence management needs to draw on the full capacity of the national S&T intellectual capital. Getting the dynamic right between those who are concerned with the operational aspects of counter-terrorism and those who deliver the S&T advice and products is a critical piece in the development of the national response framework. Flexible approaches are needed so that the laboratories with relevant expertise can be engaged quickly and directly around any evolving situation.

To achieve such agility, national S&T assets need to be linked so that research teams in related areas have established relationships and protocols, which ensure rapid coalescence of thought and action around specific incidents.

Networks of research teams, which cut across traditional organizational structures, need to be developed and exercised in preparation for specific events. These networked or virtual teams also need to work closely to advance science in areas of particular importance to counter-terrorism. Many of these areas of science have been mentioned in the paper. Defence Science needs to actively engage the new defence and security environment to ensure that the science remains focused on those aspects of defence and security that are germane to the national interest and that the defence science and technology base informs the breadth of issues that a nation must consider when addressing the terrorist threat.

Science is an essential 'enabler' in building national counter-terrorism capability. It must be carefully managed and nurtured to ensure that response communities have the equipment and tools they need, and that decision makers and policy formulators have the best scientific advice available. A strong science and technology foundation will help ensure a robust counter-terrorism capability.

"Science is an essential 'enabler' in building national counter-terrorism capability."

NOTE

This paper was originally presented at a symposium in the Netherlands, "Armed with Knowledge", 30 January 2003.

1. Paul K. Davis, "Effects Based Operations (EBO): A Grand Challenge for the Analytical Community", MR-1477-USJFCOM/AF, 2001.