



Applications of Intelligent Systems in Public Safety and Security

Study commissioned by:

precarn

*Intelligent Systems. Thinking Technology.
Systèmes intelligents. Penser technologie.*

Study conducted by:



Prepared by Actenum Corporation with Greenley & Associates Incorporated for Precarn Incorporated

Copyright © 2005 Precarn Incorporated. All rights reserved.

Public Safety and Security

This document was prepared under contract to Precarn Incorporated. Neither this document nor any part may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, microfilming, and recording, or by any information storage or retrieval system, for any purpose, without the express written permission of Precarn Incorporated.

If this document is labelled "Confidential" on this page, its contents may be neither cited nor quoted without the express written permission of Precarn Incorporated. If this document is not labelled "Confidential" on this page, permission is granted to cite or quote the contents provided the source is duly acknowledged.

Applications of Intelligent Systems in Public Safety and Security

Final Report, Wednesday, November 16, 2005.

Prepared by Actenum Corporation with Greenley & Associates
Incorporated for Precarn Incorporated.

Vancouver and Ottawa, February 2005.

Editor:

Dr. Morten Irgens, Actenum Corporation.

Annette Greenley, Greenley & Associates.

Team :

(Alphabetically)

Florissa Abreu, Actenum Corporation.

Junas Adhikary, Actenum Corporation.

Derek Best, Precarn Incorporated.

Dr. David Darvill, Greenley & Associates.

Annette Greenley, Greenley & Associates.

Dr. William S. Havens, Simon Fraser University

Dr. Morten Irgens, Actenum Corporation.

David Wright. Greenley & Associates.

Actenum Corporation is a technology and software development company specializing in intelligent systems technologies for planning, scheduling, optimization and dynamic and reactive resource allocation.

Greenley & Associates is a consulting services provider that offers clients expertise in the core service areas of Emergency Management, Human Factors, Modeling and Simulation, Project Management, and Business Analysis and Usability.

Precarn Incorporated is a Canadian national, member-owned industrial consortium supporting the development of intelligent systems technologies through its extensive network of corporations, research institutes and government partners. Precarn funds, coordinates and promotes collaborative research conducted by industry, university and government researchers.

Simon Fraser University offers bachelors, masters and doctoral degree programs to more than 20,000 full and part-time students each year. Maclean's Magazine consistently ranks Simon Fraser University among the top three comprehensive institutions in Canada.

Short Table of Contents

Executive Summary	8
Introduction.....	10
Public Safety and Security	13
Overview of Intelligent Systems	20
Challenges in PSS - Opportunities for IS	22
Intelligent Systems for PSS.....	34
Discussion and Conclusions.....	44
Appendix 1: The PSS Landscape in Canada	55
References	60

Table of Contents

Executive Summary.....	8
Introduction.....	10
Ensuring Public Safety and Security.....	10
Background and Intent of the Study.....	10
Organization of the Study.....	11
Keywords.....	12
Public Safety and Security.....	13
Trends: Skating on Thinner Ice?.....	13
Public Safety and Security as a Field.....	16
Categorization of PSS.....	17
Overview of Intelligent Systems.....	20
Challenges in PSS - Opportunities for IS.....	22
P1: Decision Support for Command and Control.....	23
P2: Training.....	24
P3: Border and Port Control.....	25
P4: Cyber Protection.....	26
P5: Smart Assistants and Communicators for Field Operators.....	28
P6: Multi-Organization Interoperability.....	29
P7: High-Value Inspection.....	30
P8: Perimeter Control.....	30
P9: Evacuation and Crowd Control.....	31
P10: Social Network Analysis.....	31
P11: Intelligent Maps.....	31
P12: Detection and Sensing.....	32
P13: Understanding critical infrastructure interdependences and protection needs.....	32
Intelligent Systems for PSS.....	34
D1: Analytics: Knowledge Discovery and Data Mining.....	35
D2: Knowledge Based Systems / Expert Systems.....	36
D3: Operations Intelligence.....	37
D4: Intelligent Simulation, Training and Tutoring.....	38
D5: Machine Learning and Adaptive Systems.....	40
D6: Intelligent Human-Computer Interaction.....	41
D8: Speech Recognition.....	41
D9: Robotics and Autonomous Systems.....	42
D10: Natural Language Processing and Generation.....	42
D11: Ambient Intelligence and Wearables.....	43
Discussion and Conclusions.....	44
Trends in Science and Technology.....	44
Overall Conclusions.....	48
Recommendations.....	50

Intelligent Systems for Public Safety and Security

Appendix 1: The PSS Landscape in Canada	55
Characteristics of PSS in Canada.....	55
Key Guidelines for PSS in Canada.....	57
Critical Infrastructure Protection in Canada	59
A Note on the PSS landscape in the United States.....	59
References	60

Executive Summary

The field of Public Safety and Security (PSS) includes a wide variety of areas within the framework of preparedness, response, recovery and mitigation; including national workplace safety, protection of critical infrastructures, and preparation and responses to avian influenza, earthquakes, wildfires, hospital viruses, insect infestations, denial of service attacks, computer viruses, and intentional malice (crime and terrorism).

The field is under mounting pressure from increasing vulnerabilities, threats and incidents. Several global trends indicate this, including an increase in natural incidents and disasters, infectious diseases, transnational crime, and terrorism. The challenges cross the spectrum of politics, economics, technology, defense and ecological affairs, and they combine and intertwine. Risk is increasing with the growth of urbanization and is compounded by large and complex critical infrastructure networks and interdependencies.

As is frequently the case when decision makers confront complex and challenging problems, the science and technology community is being called upon. This document presents the results of a study commissioned by PRECARN to investigate the current state-of-the-art of applying Intelligent Systems (IS) technologies in the area of PSS with special attention to Canada, and determine future trends in IS in of potential use for PSS. The objective of the study is to inspire researchers, technology developers, government, private industry and non-government entities involved in PSS to enter discussions and partnerships with the aim of finding practical solutions to some of the complex needs in the PSS sector.

A problem with this study is that both Public Safety and Security and Intelligent Systems are large and diverse disciplines. However, the many spheres that PSS and IS encompass present both challenges and opportunities when they are merged into an inter-disciplinary area.

Intelligent Systems may be unique in its promise to contribute to finding workable solutions to complex problems while increasing productivity and efficiency. Intelligent Systems is often described as comprising the sub fields of Intelligent Computation, Human-Machine Interface, Robotics and Machine Sensing. The field has brought us technologies for decision support in complex and dynamic environments, computer vision, autonomous vehicles, machine learning, data mining, knowledge representation, automated reasoning, and natural language understanding. These technologies may have numerous useful applications in PSS, and IS could quite possibly revolutionize preparedness, response, recovery and mitigation strategies in PSS.

Expanding the design of critical infrastructure, enhancing early detection and warning systems, improving command and control systems and developing long term management systems which incorporate lessons learned for effective preparedness and prevention are potential activities in this intersection. Intelligent Systems has the potential to enable us to plan for, manage and recover from incidents more efficiently than before, and is thus likely to enhance elements of decision-making in PSS. Application areas of IS that have been identified as applicable to PSS include: Intelligent Training and Tutoring; Machine Learning and Adaptive Systems; Intelligent Human Computer Interaction; Computer Vision; Speech Recognition; Robotics and Autonomous Systems; Natural Language Processing and Generation; and Intelligent Wearables.

PSS will meet incredible challenges and technology will be increasingly applied to address the challenges. However, the nature of threats and vulnerabilities in the field of

Intelligent Systems for Public Safety and Security

PSS makes tools and processes that are based on technology part of the challenge. Reliance on technology is in fact increasing the risks in certain PSS scenarios. A power failure or a cyber attack could greatly restrict the management and surveillance of critical infrastructure or the collection and dissemination of information for command and control decision making.

Recommendations of this study include to: encourage an R&D program co-managed by a technology organization (e.g. PRECARN) and a subject matter organization (e.g. PSEPC¹ and NSD²); support industry collaboration, multiple stakeholder teamwork and interdisciplinary research; encourage a military-to-PSS technology transfer program; move towards peer-to-peer organizational and technological networks³ and ensure that technological solutions support such networks; facilitate the collaboration and sharing of information both within and across government and industry; and to develop R&D programs that are more “demand-pull” than “tech-push” to ensure that technologies will be developed from real needs and address real problems.

¹ Public Safety and Emergency Preparedness Canada.

² The National Security Directorate.

³ Peer-to-peer networks are much harder to incapacitate, as each node in the network operates on a peer level with any other node.

Introduction

Ensuring Public Safety and Security

The field of Public Safety and Security, which this report refers to as PSS, is large and diverse. It includes a wide variety of issues, such as a nation's workplace safety, protection of critical infrastructures, response to avian influenza, earthquakes, wildfires, hospital viruses, insect infestations, denial of service attacks, computer viruses, and intentional malice (crime and terrorism). Hence, PSS is no longer only just about providing fire trucks and emergency wards for hospitals. Nor is it only about emergency operations centers and field workers. Now there are many government, private industry and non-government entities engaging with the traditional first responder communities (such as fire, police and emergency medical services) to provide protection for individuals and the nation state as a whole. "Public Safety and Security" is a term that is more widely used in Canada; in the United States, much of this work can be found under the term "Homeland Security".

In recent years, especially since September 11, 2001, greater attention is being paid to PSS. This focus is creating an evolution of decision-making and communication strategies in governments, private industry and non-government organizations. In turn, these entities are increasingly asking research institutions and the technology sector for help, including the area that is known as "Intelligent Systems".

"Intelligent Systems" (in this document referred to as IS) is also broadly defined. It is often described as comprising the sub fields of Intelligent Computation, Human-Machine Interface, Robotics and Machine Sensing. The intelligent systems field encompasses many diverse areas where tools have been developed to communicate, learn, respond and act in environments to aid the human user, such as decision support, computer vision, autonomous vehicles, machine learning, data mining, knowledge representation, automated reasoning, and natural language understanding – to name a few.

PSS is under mounting pressure, and as is frequently the case when decision makers confront complex and challenging problems, the science and technology community is being called upon to contribute to national goals. In this case, the question is how IS technologies can help the PSS sector to overcome its challenges.

Background and Intent of the Study

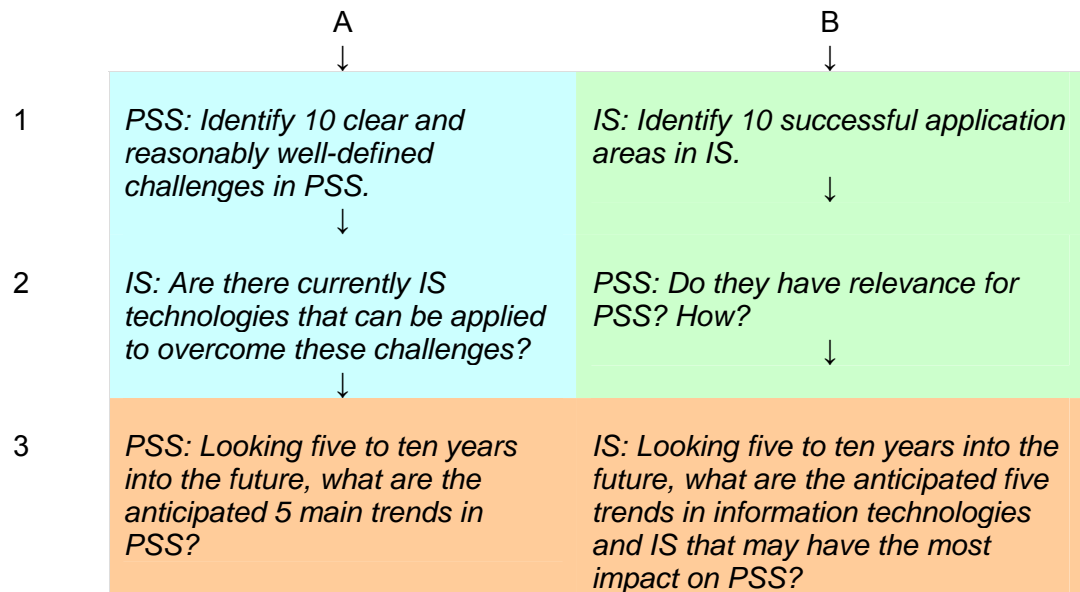
This document is commissioned by Precarn Inc., which is a member-owned, not-for-profit industrial R&D network supporting the development of IS technologies in Canada. The document is part of a study where the objectives are to 1) investigate the current state-of-the-art of applying IS technologies in the area of PSS with special attention to Canada, and 2) determine future market and technology trends in IS in the area of PSS.

This document provided the basis for a discussion at a workshop that was held in Ottawa on January 20th, 2005 and includes input from the participants during the workshop. The study will, at a minimum, raise awareness of the issues. The objective of the study is to inspire researchers, technology developers, government, private industry and non-government entities involved in PSS to enter discussions and partnerships with the aim of finding practical solutions to some of the complex needs in the PSS sector.

Organization of the Study

Due to the fact that both the PSS and IS fields are wide and diverse, it has proven difficult to provide a comprehensive overview of their mapping in a short study. In order to add structure and focus and enable the analysis of the two fields, the study has used a framework that has as its aim to highlight the abilities of IS and the needs of PSS.

The following discussion outlines the process that was used. The process was developed with two tracks, called Track A and Track B, where Track A was based on the needs in the PSS field, and Track B was based on the abilities of IS. Each track had three tasks:



Subject matter experts (SMEs) in the fields of PSS and IS were approached via interviews and/or were engaged in a discussion during the workshop based on this framework.

This document is organized as follows:

1. *Part 1, "Challenges in PSS – Opportunities for IS", discusses A1 and A2.*
2. *Part 2, "Intelligent Systems for PSS", discusses B1 and B2.*
3. *Part 3, "Discussion and Conclusions", discusses A3 and B3.*

Prior to the workshop and the conduction of interviews with SMEs, the discussion paper put forward PSS challenges (task A1) and potential IS application areas (task B1) to be considered as starting points for discussion. SMEs were engaged during interviews and through workshop participation to verify and validate the initial findings of this study.

In line with the framework developed above, this document attempts to exploit the potential for relationship from both the PSS and IS point of view. Part 1 examines potential areas in PSS where IS may provide support, and Part 2 examines areas of IS that may be relevant for PSS.

Keywords

Emergency Management; Critical Infrastructure Protection; Public Safety and Security HAZMAT; Disasters; Terrorism; Technology; Decision Support Systems; Intelligent Systems; Modeling; Simulation; Artificial Intelligence; Information Technology; and Interdisciplinary Research

Public Safety and Security

Trends: Skating on Thinner Ice?

Are we skating on thinner ice? It seems public safety and security vulnerabilities, threats and incidents are increasing at an alarming rate. Several trends indicate this, including an increase in natural incidents and disasters, infectious diseases, transnational crime, and terrorism. The challenges facing our societies cross the spectrum of politics, economics, technology, defense and ecological affairs. Furthermore, they combine and intertwine. Risk is increasing with the growth of urbanization⁴ and is compounded by large and complex critical infrastructure networks and interdependencies.

Ecological Stress

During the past century, world population grew by more than 4 billion - three times the number of people when the century began. At the same time, the use of energy and raw materials grew more than ten times [WWI 1999]. The environmental cost of food production is starting to take a toll, for instance does the salmon waste off the B.C. coast release as much nitrogen as sewage from a city of 250,000 [Eilperin 2005]. Of the 242,000 plant species surveyed by the World Conservation Union in 1997, some 33,000, or 14 percent, are threatened with extinction, mainly as a result of massive land clearing for housing, roads, and industries. This mass extinction is projected to disrupt nature's ability to provide essential ecosystem services, ranging from pollination to flood control.

Natural Disasters

2004 was marked by the catastrophe on 26 December, when a strong seaquake hit the north of Sumatra and triggered seismic sea waves that surged with great force against sections of coast a great distance away. Nearly 300,000 people were killed and millions more were made homeless. However, even before the seaquake, 2004 was already the costliest natural disaster year ever for the insurance industry [Munchener]⁵. The last ten years have witnessed an increased number of natural and technological disasters that have killed 478,100 people, impacted the lives of more than 2.5 billion people and caused about US\$690 billion in estimated economic losses. The frequency of natural catastrophes more than doubled between 1960 and 2003 [Munchener]⁶. The rate at which the occurrence of natural disasters is increasing is shown by the fact that in the year 2003, there was an almost constant increase in the number of natural catastrophes from one month to the next⁷.

⁴ As illustrated by the accident in Bhopal.

⁵ This includes losses of US\$ 40bn with cyclones in the United States, the Caribbean, and Japan alone causing death and destruction, and generating insured losses exceeding US\$ 35bn. Even before the December seaquake, natural catastrophes had already claimed over 15,000 fatalities in 2004. The Caribbean was hit by two severe catastrophes. In May, flash floods and flooding claimed over 2,000 lives in Haiti and the Dominican Republic. In September, Hurricane Jeanne devastated the two countries, with again almost 2,000 victims. On 24 February, an earthquake that rocked the north of Morocco killed 640 people.

⁶ Economic losses had by the end of 2003 increased by a factor of 6.7, and insured losses by a factor of 13.5 (for a total of US\$ 187bn in 2003).

⁷ Of the 700 events occurring throughout the world that year, 43% were due to windstorms, 28% to floods, 17% to other events, and 12% to earthquakes and volcanic eruptions [Munchener].

For instance, the pine needle beetle infestation in BC, which is attributed to milder winters, has killed an area so large that it is easily visible from the space station. The percentage of the Earth's land area stricken by serious drought more than doubled from the 1970s to the early 2000s, and widespread drying is occurring over parts of Canada, Europe, Asia, western and southern Africa, and eastern Australia [NCAR]. The consequences are numerous. Thousands of villagers in Kenya's central Rift Valley fled their homes in February 2005 after 15 people were killed in clashes over water rights [Agence France 2005]. The year 2003 was the worst year of forest fires in BC's history, losing 26,4747 hectares, or more than 11 times the average over the ten years before⁸. The excess mortality in France during the heat wave in August 2003 was more than 11,000, equivalent to a total mortality increase of 55%⁹ [InVS 2004]. The level of unpredictability in natural disasters is further illustrated by the fact that not only have droughts afflicted the global population with increasingly disastrous consequences, but so have excessive amounts of rainfall. As the average global precipitation has risen¹⁰, major floods across the globe in the 1990s caused economic losses exceeding US\$ 200 billion. Whereas only six major flood catastrophes were recorded in the 1950s, there were no fewer than 26 in the 1990s [Munchener].

Technological Disasters

The most infamous technological disasters are probably the release of 30 tons of methyl isocyanate (MIC) at the Union Carbide pesticide plant at Bhopal, India (killing 2,800 people and causing respiratory damage and eye damage to over 20,000 others), and the core meltdown of the nuclear reactors in Chernobyl nuclear plant, Ukraine in 1986 (necessitating the evacuation of 135,000 people and causing a sharp increase of thyroid cancer in the area). Canada has several risk points, including nuclear generation plants, oil transportation from Alaska and offshore installations. Large-scale technological disasters have not happened in North America, but there are indicators that with the increase of asymmetric adversary tactics and our reliance on technology, threats and vulnerabilities, and therefore risk, have increased.

Infectious Disease

Infectious disease represents a growing threat to individual and national security, because of the emergence of new illnesses¹¹; the increasing inability of modern medicine to respond to resistant and emerging pathogens; and the growing threat of bio-terrorism and bio-warfare¹². In Canada, cattle producers have lost about \$5 billion since the discovery of one animal with mad cow disease in the spring of 2003 [BMO 2003], while the United Kingdom estimated that its outbreak of foot-and-mouth disease resulted in over US\$10 billion in losses to tourism and the food and agriculture sectors (including the slaughter of over 4 million animals) [GAO-04-259T 2003]. The direct cost of human infectious and parasitic diseases in Canada was estimated in 1993 at \$3.385 billion¹³. A considerably bleaker example is the impact of the HIV / AIDS epidemic in southern Africa. In the region, the chance is about 50-60% that a teenager will contract HIV

⁸ And also four times its annual fire suppression budget.

⁹ The heat wave and its associated forest fires in Europe in 2003 is the single most costly disaster of the last ten years, with an estimated damage of US\$ 13 billion and more than 32,000 deaths.

¹⁰ The warmer global climate is increasing the overall land area experiencing either very dry or very wet conditions.

¹¹ Such as Acquired Immune Deficiency Syndrome (AIDS), Ebola, and hepatitis C.

¹² In addition, human actions amplify these trends by putting us in ever-greater contact with deadly microbes. Globalization, modern medical practices, urbanization, climatic change, and changing social and behavioral patterns all serve to increase the chance that individuals will come in contact with diseases, which they may not be able to survive.

¹³ Direct costs accounting for approximately \$785 million and indirect costs accounting for nearly \$2.6 billion.

during his or her lifetime, and those on the threshold of adulthood today can expect just 15 or 20 years of adult life ahead of them. As a result, not only is the economy shaken, but also the pillar institutions of the societies, as fewer people live long enough to fill senior positions and contribute as working members of a society that increasingly needs assistance outside of the family unit to support the young, the aged and the terminally ill.

Non-State Actors, Terrorism and Transnational Crime

Targeting terrorism at its source is an appealing notion. Unfortunately, the enemy is not cooperating. There is no central front on which they can be cornered and destroyed.

National safety and security was previously a question of war and peace. However, war has now been replaced by concerns for nontraditional challenges — so-called “gray area phenomena”. We have seen a clear trend over the last ten years towards an increased fluidity in international politics. The new geopolitical landscape lacks the relative stability of the Cold War division between East and West, and the definitions of security, conflict, and general threat are becoming diffuse. Globalization has increased the quantity and speed of trans-national trade, which presents further confusion in an environment where risks are not clear cut and it is no longer apparent exactly what can be done to whom and with what means¹⁴. As a result, public safety and national security, which always have been strongly related, have become more difficult to separate¹⁵.

Democratization of Knowledge

A risk-increasing trend is democratization of knowledge. Legislation and mechanisms such as the Internet help to facilitate accessibility, as access to information is progressively more being regarded as a democratic right. Information that is put into the public realm for good-will purposes or to foster inclusive agendas of political systems, can also be used maliciously by adversaries. For example, the Federal Aviation Administration (FAA) provides a conveniently downloadable map on the Internet of numerous other sites, called “temporary flight restrictions” that includes nuclear power plants, national laboratories, and even the president’s ranch¹⁶. “The Terrorist’s Handbook”, which you can find on the Internet, will tell you how to build bombs and how to make the explosives that go into them¹⁷. In 2003, a passenger on a trans-Atlantic flight tried to light up a bomb in his shoe that he had build by following a recipe he found on the Internet¹⁸. In addition, municipalities provide interactive city maps and emergency

¹⁴ In 1984, a sect poisoned salad bars in Oregon with salmonella bacteria, causing 750 persons to become ill. In the last ten years, we have seen the release of neurological gas in a Tokyo subway, the ramming of passenger jets into civilian buildings and attacks on schools and children. This trend is sometimes described as “from mad to nuts”.

¹⁵ The commuter train bombings in Madrid in March illustrate that terrorists are living and operating within jurisdictions of Canada’s allies and do not need to receive aid and comfort from rogue states. According to the U.S. Department of State’s latest revised global terrorism report, the number of terrorist incidents went up in 2003, despite the U.S.-led invasions of Afghanistan and Iraq.

¹⁶ Another example is that up until a year ago, you could download from the Internet a map of the unprotected pumping stations along the Alaska pipeline.

¹⁷ It will also tell you how to acquire them elsewhere: just walk over to the chemistry laboratory at any nearby university, go into the stockroom, and load up your backpack with all the ingredients you need to make high explosives.

¹⁸ What the passenger, Richard Reid, had prepared was triacetone triperoxide, or TATP. It can be made from hydrogen peroxide, which you can buy from the local pharmacy; acetone— not the type for fingernails, but the paint-thinner variety available in any hardware store; and a small amount of hydrochloric acid (sulfuric acid will also do). You can find several procedures on the Internet for combining these ingredients to synthesize TATP. What Richard Reid didn’t know, as he tried to strike a match to ignite his TATP-lined shoes, was that it’s shock-sensitive. If he had simply stamped his foot, he and the plane might have been history.

response plans for the diverse and multiple stakeholders that are engaged in community level programs.

Sociological Change

In developing countries, the average number of births has fallen from 5.9 in the 1970s to 3.9 in the 1990s [BBC News 2005]. Low birth rates also impact the economic and health sectors of nations. In 1945, the ratio of workers to retirees in United States was over 40 to 1; in 1950, over 16 to 1; and in 1960, the ratio was 5 to 1. Today, the worker/retiree ratio is a little over 3 to 1 [Muehlencamp 2005]. In 2050, the ratio of workers to retirees will shrink to 2 to 1 and 80.1 million Americans will be over age 65. Barring a cure, 14 million Americans will have developed Alzheimer's Disease [NIA 2050]. These trends may have a profound impact on public safety and national security.

Complex, Interdependent and Vulnerable Critical Infrastructures

There are many recent events that can be recounted to illustrate the growing complexity, interdependency and vulnerability of critical infrastructures. On August 14, 2003, the largest power blackout in North American history affected eight U.S. States and the Province of Ontario, shutting down more than 20 power generators (including nine nuclear reactors) and leaving up to 50 million people with no electricity [NRC-USDE 2004]. An outbreak of hepatitis at restaurants in four U.S. states in 2004 that killed three people and infected more than 600 was traced to green onions imported from Mexico. Poor control routines around the drinking water of the town of Walkertown in 2002 caused an E. Coli outbreak that killed seven and made half the town's 5,000 residents ill [Walkerton-2005]. In January 2003, 92 people became ill after buying ground beef from a Michigan supermarket that was intentionally contaminated with nicotine [GAO-04-259T 2003]¹⁹. The USDA calculated that a foot-and-mouth disease outbreak could spread to 25 states in as little as 5 days [GAO-04-259T 2003]²⁰. And these are just a few examples of complex and vulnerable critical infrastructures that include food and water, telecommunications, gas and oil (and their related upstream, downstream and midstream activities of exploration, refining, storage and transportation), transportation, banking and financial services and emergency-service institutions, including hospitals, police stations, fire and rescue departments.

The complexity and speed of events and the severity of global environmental and political stress are believed to be soaring [Homer-Dixon-2000]. The illustrations above are just some examples of where and why modern societies see increased risk. More than anything, it illustrates the complexity of key elements involved in ensuring public safety and security.

Public Safety and Security as a Field

Public Safety and Security (PSS) is a function of interaction between municipal, provincial, federal and international government agencies, private industry, non-government organizations (NGOs) and members of the public to protect citizens and critical infrastructures. It is assumed in this report that PSS is focused on preparing for, avoiding and reacting to incidents. An incident is defined as either a naturally caused or

¹⁹ A highly contagious and, for poultry, deadly strain of avian influenza on a Texas farm also spread to live bird markets in Houston.

²⁰ Cattle remains are being fed to chickens, whose remains can be fed back to cattle, increasing the probability of spreading disease while making tracking difficult.

human initiated (accidental or intentional) event that threatens the safety or security of individuals or the critical infrastructures vital to the nation as a whole. The most common incident management framework used in the first responder field is *preparedness, response, recovery and mitigation*. This framework is applicable to the diverse activities that are necessary in a number of the public safety areas as defined by Public Safety and Emergency Preparedness Canada (PSEPC).

The most frequent PSS incidents are common fire, police and medical incidents. In general, the procedures for handling these events are usually routine. However, other PSS incidents can range from relatively infrequent, but potentially catastrophic, natural events (such as floods, wildfires, famines, epidemics, storms, avalanches or earthquakes) to a wide range of human initiated events, whether accidental (e.g., from air, marine, road or rail accidents to lost persons) or possibly planned (e.g., road or area closures or terrorist events). As most PSS incidents start off as local incidents, the local agencies are typically first on the scene, which are then supported by provincial, federal and/or international agencies as the incident evolves.

Traditionally, the public safety and security field has been regarded as to be in the realm of fire, police and emergency medical services (EMS). More recently, there has been an increasing focus on critical infrastructure protection (CIP). Critical infrastructures provide the necessary backbone for our nation to run. With the onset of the information age, just-in-time operations, massive urbanization, interdependent organizations, networked linkages and increased complexity of technologies; these infrastructures have become more interdependent as society has become more reliant upon them. The interruption of their service provision increases the vulnerability of society to any threats to their operational capability. In this regard, while traditional PSS concerns were linked to protecting the individual, this new focus places PSS emphasis on protecting the nation as a whole.

Categorization of PSS

The following discussion outlines some of the familiar ways PSS is categorized. This delineation helps to provide some structure for the complexity of the components that are characteristic to the field.

PSEPC's Categorization of Public Safety

The areas of Public Safety in Canada as defined by PSEPC includes: *criminal activity/policing, environment, financial safety, internet safety, product/consumer protection, transportation and travel safety, emergencies, family and home safety, health, national safety and security, recreational safety, and workplace safety*.

This list illustrates how broad and dynamic the field of PSS is. As emergencies are just one component of the field, it was critical that efforts in this study were not limited to focusing on PSS activities related to emergency response. This approach is especially important in studies that are concerned with research and development to ensure that technological solutions are applied in alignment with user needs.

Categorization of PSS within the Incident Management Framework

Incident management organizations in Canada have widely accepted the framework of Preparedness, Response, Recovery and Mitigation for emergency management:

1. **Preparedness** - Preparedness involves planning, training, exercising, procuring and maintaining equipment, and designating facilities for emergency purposes. Preparedness activities improve the ability to respond quickly and efficiently in the aftermath of an incident and apply lessons learned from post incident investigation findings.
2. **Response** - Response activities occur immediately after the onset of a disaster—that is, during the initial impact of a disaster. Response involves carrying out time-sensitive actions to save lives and protect property during an emergency or disaster. The Incident Command System (ICS) is one of the organizational approaches used to coordinate resources and multiple agency decision-making during the response phase.
3. **Recovery** - Recovery activities begin after the initial impact of the incident. They can be broken down into short-term and long-term activities and are geared towards returning all systems to pre-incident status. Recovery activities can continue long beyond any “state of emergency” period that immediately follows a disaster. Business continuity is also a key aspect of the efforts extended through recovery activities.
4. **Mitigation** - Mitigation is often seen as the cornerstone of emergency management. Mitigation involves incident avoidance and incident detection activities that prevent a disaster, reduce the chance of it happening, or reduce its damaging effects.

Categorization by What is Protected

- *Individual citizen*
- *Critical infrastructure*

There is increased recognition that critical infrastructure is not only one of many elements of PSS, but a prime area that provides the capacity for the stakeholders in the PSS field to protect individuals. For example, without infrastructure such as roads, utilities, and communication links, the ability for police, fire and EMS organizations to protect individuals is significantly compromised.

Categorization by Source of Incident

This study has identified three different originating sources of PSS incidents:

1. *Natural incidents*
2. *Human accidents and human error, and*
3. *Antagonistic incidents and malicious attacks that are human initiated.*

Categorization by Operation Level of Activities

This study has identified three different operational level of activities in the field of PSS:

1. *Strategic* – i.e., senior management engage in high-level decision making and planning activities. Influences such as legislation, policy and the nature of inter-agency collaboration will impact the context of their approach to PSS.

2. *Operational* - i.e., Incident commanders employ the strategic directives while implementing plans, allocating resources, monitoring activities and assessing the PSS environment.
3. *Tactical* - i.e., Field workers and on-site responders execute the activities required to facilitate the necessary protection to individuals and critical infrastructure, and to realize the strategic objectives.

These three levels are interdependent yet have their own unique requirements for decision-making and coordination. The needs of field workers are very different than operational managers or strategic planners. These differences have an important impact on which technologies and tools are required. For instance, field workers require high-quality and reliable communication links with each other and their incident commander when engaged in response and recovery activities that can overcome challenges such as the inability to operate small devices while wearing protective clothing that leaders at the strategic level do not face. Carrying devices with embedded smarts facilitate their connectivity and provide an opportunity for tools that offer multi-modal technologies, such as voice, visual and various touch activation capabilities.

Overview of Intelligent Systems

Intelligent Systems (IS) technologies have had broad impact across the globe. For example the world's most popular search engine, Google, uses IS technologies to respond to millions of queries a day; banks now depend on IS to alert customers to odd patterns of credit card use; the gaming industry depends on this technology to develop life-like characters; IS components are embedded in numerous devices, such as photocopier machines to maintain copy quality; IS are in everyday use for tasks such as configuring products, aiding complex planning tasks, and advising physicians; IS are playing an increasing role in corporate knowledge management in facilitating the capture and reuse of expert knowledge; IS are also increasingly being used in defense and PSS. This endless list helps to illustrate the diverse areas that encompass the field of IS.

Due to the wide range of applications that have been developed in the field of IS, the field is broadly defined. The IS field is often considered to be concerned with the design and analysis of artificial autonomous agents (software systems or physical machines) that are able to communicate, learn, respond and act in environments to aid the human user. In the field of PSS, software systems may be found embodied in decision support systems for command and control, "smart" PDAs for first responders, and intelligent tutoring and training systems. As physical machines, they may be embodied in small robots and autonomous vehicles, equipped with sensors and actuators. One way of classifying the field is using the following four components:

1. *Intelligent Computation* - This area includes sub-fields, such as knowledge-based and reasoning systems, neural networks, fuzzy logic, data mining, intelligent scheduling and machine learning.
2. *Human-Machine Interface* - This area includes human factors and user-centered design, speech/sound recognition and graphic displays.
3. *Robotics* - This area includes actuation, controls, tele-operation and simulation.
4. *Machine Sensing* - This includes vision, tactile and position/motion/force.

An intelligent system has to act rationally towards its tasks, and to interact with other agents, with human beings, or its environment. IS is thus related to the field of Artificial Intelligence (AI). AI, despite its unfortunate name, is about natural and artificial information processing systems – and thus about how information is acquired, processed, stored, used, etc., in animals and machines.

The size and diversity of the field obviously creates overlaps with several disciplines, including, psychology, neuroscience, logic, linguistics, mathematics, cognition, biology and philosophy. However, for the purpose of this study, we are mainly interested in the functional, engineering and usability aspects of Intelligent Systems. We will define the scope of this study for Intelligent Systems in the next section.

Within this narrower focus, AI is still a wide field, focused on studying the computational requirements for tasks such as human perception, reasoning, and learning, and develop systems to perform those tasks. The fields are concerned with topics such as computer-based problem solving, decision support, learning, general and specialized knowledge representations, search algorithms, reasoning mechanisms, computer vision, planning and acting, robotics, multi-agent systems, speech recognition, and natural language understanding.

Intelligent Systems for Public Safety and Security

IS is also concerned with emerging advanced technologies that are not a traditional part of AI. These technologies may also be relevant to PSS. Examples include work in artificial life, emergent behavior, games, wearable computers, context traces and ambient intelligence.

The size and diversity of the field obviously creates overlaps with several disciplines, including, psychology, neuroscience, logic, linguistics, mathematics, cognition, biology and philosophy. However, for the purpose of this study, we are mainly interested in the functional, engineering and usability aspects of IS. We will define the scope of this study for IS in the next section.

Challenges in PSS - Opportunities for IS

Areas requiring long-term research to support national needs in responding to threats of terrorism may include:

1. An improved ability to prevent incidents by systematically reducing vulnerability while increasing preparedness through improved design of our infrastructure (e.g., buildings, the Internet, transportation networks, etc.).
2. An enhanced ability for early detection and warning. Examples include tsunami detection and biological, chemical, and radiological agents, disease or toxic chemicals in media such as food, water, and air.
3. An improved ability to respond and control incidents. Examples include network-based emergency response and information technology capabilities (e.g., instant messaging, database integration, data mining, system modeling) that will allow for intelligent emergency response with functioning and integrated command and control systems.
4. The development of post-event analysis systems that provide the capability for long-term management and analysis of incidents and the insight needed to improve prevention, preparedness, detection, and response in the future. This system must also support the need for public education and information dissemination.

The list above is more a classification than concrete challenges. There are many possible areas of PSS that could benefit from IS technologies. The list could be very long, including examples like force-feedback arm exoskeleton for training and rehabilitation, performance comparisons in real and simulated environments, forecasting of international conflicts, nano-scale sensors for remote sensing of chemical and biological agents, optical methods for chemical and biological threat detection, and game theory-based terrorism risk models.

Some solutions may be applicable to one specific area whereas others may be useful to more than one task, level of operation or phase of the incident management framework of preparedness, response, recovery and mitigation. In addition, a combination of technologies may offer the best solution in some instances, and in others, a single technology may be the most useful.

This study has identified the following areas of PSS where IS technologies are relevant:

PSS Areas Applicable for IS Technologies	
P1	Decision Support for Command and Control
P2	Training
P3	Border Control and Port Protection
P4	Cyber crime protection, detection and analysis
P5	Smart Assistants for Field Operators
P6	Multi-Organization Interoperability
P7	High-Value Inspection
P8	Perimeter Control
P9	Evacuation and Crowd Control
P10	Social Network Analysis
P11	Intelligent Maps
P12	Detection and sensing
P13	Infrastructure Protection
P14	Event detection
P15	Deception detection
P16	Web-based intelligence monitoring, mining, and visualization
P17	Crime and intelligence visualization
P18	Bio-terrorism tracking, alerting, and analysis
P19	Major (natural and manmade) disaster prevention, detection, and management
P20	Criminal data mining

Thirteen of these areas have been selected to be expended up on for this study and are described in more detail below²¹.

P1: Decision Support for Command and Control

Decision makers in command and control centers need expert tools that support gathering and extracting information, reasoning over information, and enhancing situational awareness.

Recent technological advances have facilitated an enormous increase in electronically available data from sensory networks²², digital telephone switches, the internet, and satellites as information technology systems (ie., enterprise resource planning systems, corporate intranets, GPS²³, CRM²⁴ systems, and supply-chain management systems) provide increased amounts of higher quality operational data.

²¹ There are of course many more areas where useful and interesting projects can be found, including force-feedback arm exoskeleton for training and rehabilitation, performance comparisons in real and simulated environments, forecasting of international conflicts, nano-scale sensors for remote sensing of chemical and biological agents, optical methods for chemical and biological threat detection, game theory-based terrorism risk models, and so on.

²² The science and technology plan for the Science and Technology Directorate of the Department of Homeland Security in the U.S. lays out research and development priorities. Information technologies research is prominent, particularly in the area of developing sensor networks [Merritt 2004]. Hence a lot of data will be produced.

²³ Geographical Positioning Systems.

²⁴ Customer Relationship Management.

While command and control centers of tomorrow need to be provided with constantly updated and reliable data, more data is not enough. First of all, commanders need help to find the *right* data. Too much data can actually make matters worse with what is known as information overload²⁵. Secondly, in order to help commanders increase their situational awareness, they need to be presented this information in useful, efficient and relevant formats.

If the discussion ended here, a view of decision support would be one of providing decision makers with passive (albeit correct) information. But decision support is much more. Decision making in command and control centers during PSS events are often very complex tasks, and decisions often have to be taken under time pressure²⁶. These decision makers thus need decision support tools that are active collaborators in the decision making process. The software systems need to have domain specific problem solving knowledge²⁷, where they go from providing background material for decisions to proposing which decisions could be made.

In order to efficiently support the human user in their decision-making, data needs to be complemented with an efficient means of finding the right information, an ability to reason using the information, and a capability to visualize, or model the data. The end result is layers of functions that work on the data on its way from the source to the decision maker:

1. *Layer 1: Data Gathering.*
2. *Layer 2: Data Mining: Find the right information.*
3. *Layer 3: Reasoning: Collaborate in making the decision.*
4. *Layer 4: Data Visualization: Visualize the situation and create a protocol for problem solving collaboration between the commander and the system.*

IS can assist on all four levels of decision support. Government and industry research has been actively engaged in providing the PSS sector with the necessary technologies for some of these layers, especially in the US. For example, Sensory Networks, Data Gathering and Data Mining are important focuses of the DARPA R&D program of the Department of Homeland Security in the U.S.

P2: Training

Training strategies are evolving as the field of PSS is growing and the number of threats is increasing. For example, courses offered by the US Federal Emergency Management Agency (FEMA) incorporate newer concepts of incidents involving chemical, biological, nuclear, radiological, toxic industrial material and explosives agents as pre-meditated weapons rather than accidental disasters caused by human error. This training addresses gaps in the traditional educational system. For example, health care professionals are not accustomed to being trained on Anthrax or Sarin in medical school.

²⁵ The amount of all information ever produced, beginning when man first painted pictures on cave walls and wrote on papyrus, is estimated to a total of 18 exabytes ($2^{60} = 1,152,921,504,606,846,976$, or roughly 10^{18} bytes). Yet 12% of the information was produced in 1999 alone, two thirds of that being digital [PORT, 2001]. Statistics gathered by IDC show that the average human can only read about 300KB of text per hour without analyzing it [Schwartz 2001].

²⁶ Highly complex tasks under time pressure with possibly serious consequences of the decisions may be compared to playing speed Chess with a gun to your head.

²⁷ For instance medical diagnosis, resource reallocation, feasibility analysis and fire development analysis.

David Cox, M.D. a program manager for the Urban Security Initiative of the National Medical Response Team, WMD Central in Denver, Colorado, is involved with training hundreds of first responders in the US. In an interview for this study, he outlined that one of the challenges of PSS is training the medical community to vaccinate hundreds, if not thousands, of people. In addition to procedural training, the community needs to determine how best to access the national medical stockpile in an environment that lacks standardization across jurisdictions.

Cost, media attention, and security risks hinder training exercises involving multiple agencies. The result is that training is done much too seldom, if ever and that standardization across jurisdictions is scarce or non-existent. By using modeling and simulation tools, exercise scenarios can be played out over and over again, educating multiple users on various agents and the roles and responsibilities of the collaborating agencies in a cost-efficient mechanism that promotes standardization.

IS Technologies can play an important role in providing the necessary sophistication to training and tutoring systems. Technologies from Emergent Behavior and Artificial Life have been used with great success in creating sophisticated and believable simulation environments²⁸. Intelligent Tutoring Systems (ITS) is a field of IS that have been around for several years. ITS can manage the learner's experience with PSS models, visualizations and procedures in order to ensure the most effective possible pedagogical experience for an individual learner. Introducing the possibility of ITS training with other live participants on-line, or with IS agents acting as other participants, can provide an effective learning environment that includes training for common PSS scenarios and procedures as well as for high risk unlikely, but potentially catastrophic, scenarios.

P3: Border and Port Control

A nation's borders have always been seen as a vulnerable point, however much has changed in this domain since the end of WWII, and especially with the fall of the iron curtain in the former USSR, leading to the end of the cold war. Globalization and the expansion of the market economy into the former USSR, South-East Asia and beyond has opened national borders to goods and people, both legal and illegal, in greater numbers than ever before. The development of transportation linkages and increased traffic of trade coupled with the increased movement of people and the growth of multinational immigrant populations in western societies have presented new challenges to border control and port protection. In addition, adversaries who threaten a country's national security are no longer other nation-states. Lone actors or members of small groups with ill intentions are more difficult to detect than an army arriving on one's doorstep. Narcotics, disease, illegal immigrants, terrorists and unconventional weapons, all enjoy easier passage than ever before. Unfortunately, fortifying the frontiers is not a solution. It would not only slow down trade and impact economies negatively, but would also create political challenges on the international stage with accusations of "protectionism".

Challenges in border control and port protection include:

1. *Inspection of passengers and their baggage.*

²⁸ These technologies have been used to great effect in animation, for instance the battle scenes in the "Lord of the Rings" movie trilogy.

2. *Inspection of commercial shipments on air, land and sea carriers.*

3. *Intelligence gathering and collaboration with foreign countries.*

The screening and detection of people, objects and substances being illegally transported across borders is a daunting task, mired with all kinds of controversy including human rights, privacy and national security. The diverse cultural norms in the international community regarding these domains only make intelligence gathering and collaboration even more complex as security and protection issues cross into the political sphere, no longer just a process of trade and commerce.

Inspection is a resource intensive act that typically is happening at random intervals at a nation's entry points. The most effective method for inspection is to inspect everything and everyone. This is of course not feasible. The challenge is to find methods of inspection that have the largest effect and the lowest cost. Screening and detection tools have a great propensity to aid in this domain, applying technologies to reduce the manpower involved while increasing the level of surveillance.

Information technologies and IS can help border control keep pace with booming commerce. For example, observing, tracking and controlling are the current primary means of providing port and border security. With the amount of traffic at some of Canada's busiest ports, a system to track and direct vehicles, whether they be planes, trains, trucks or ships. Automated systems allow for easier detection of vehicles not following directives or displaying atypical behaviour. Cargo screening and detection of hazardous materials at entry points may also benefit from the development of IS tools with sensors and analytical capabilities that could react faster than a human baggage attendant or forklift driver. These high-tech systems can increase the quality of inspection activities with fewer resources, thus providing further cost benefits.

P4: Cyber Protection

Information technology increasingly pervades the operations of weapons systems, national economies and infrastructures, including the control of electric power grids, transportation networks, and water supplies. The rapid proliferation and integration of telecommunications systems and computer systems has resulted in a complex network of interdependence. This inter-linkage, combined with an emerging constellation of threats and vulnerabilities, poses unprecedented risk. As a result, cyberspace has become the Achilles heel of modern nations.

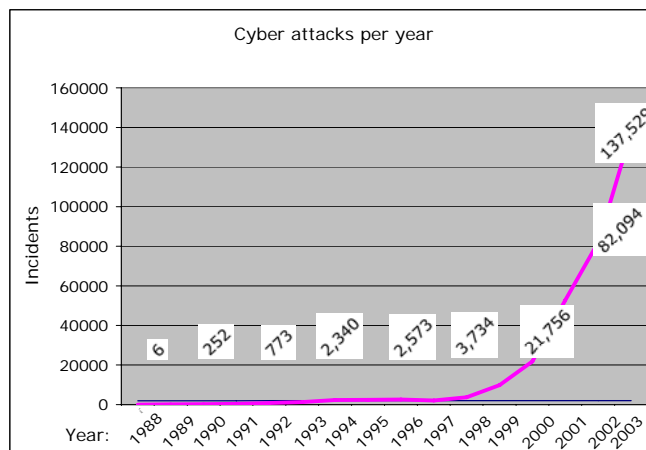
The ability to respond to PSS events is increasingly dependent on technology and communication. As the number of information technology tools being applied to operational and strategic concepts grows²⁹, and activities of command and control center operators, emergency planners and first responders are increasingly becoming dependent on it. For example, the Canadian Meteorological Centre of Environment Canada has simulation programs that run over 1,000,000 lines of codes each. Running these simulations provides critical information essential to predicting the effects of

²⁹ This is of course also the case for national defense forces, which increasingly are dependent on technological superiority for military doctrines – for instance plans ranging from computer-based weapons research programs to software that encrypts classified military data, from computer-guided "smart" bombs to a space-based missile defense.

weather on Canadian and international areas of concern³⁰. Protecting this information and ensuring its availability is important to all Canadians.

Science and technology have always provided humanity with a double-edge sword. As technologies have become increasingly sophisticated, threats of their abuse have grown. The information warfare being waged today involves information snooping and computer sabotage by hackers acting on behalf of individuals, groups or governments³¹. Thus, the reliance on technology is not only beneficial to the realm of PSS, but it also enlarges the areas of risk, making cyber-attacks an increasingly attractive and effective weapon.

Protection of Nodes: Cyber protection is important not just due to the amount of havoc a virus or a hacker can cause to a network. As centralized command and control centres have gained in popularity, the need to ensure the uninterrupted ability to program, monitor and control equipment remotely is key. Power plants, nuclear facilities, water treatment plants, factories and government agencies have implemented internet-based technologies over the past several years for remote monitoring and control of the facilities using web browsers. As national critical infrastructures have become increasingly reliant on information technologies such as the Internet, their vulnerabilities have been exposed as they have been subjected to sabotage and denial of service attacks. More than 130,000 online cyber attack incidents were tracked in 2003, which is six times higher than in 2000³², which can be seen from the figure below³³.



Another area of concern is the ability for systems to accurately detect when there is unauthorized access. A Vice-President of Information Technology for a Fortune 1000 company interviewed for the study indicated that one of his greatest challenges was there were too many false positives (meaning the system believes it under attack, when

³⁰ As discussed in an interview with Jean Michel, Director of the Operations Branch The Canadian Meteorological Centre, Environment Canada, December 2004.

³¹ The recent escalation of tension between Israel and the Palestinians, for example, has had a prominent virtual dimension. From October 2000 to January 2001, attacks by both sides took down more than 250 Web sites, and the aggressions spread well beyond the boundaries of the Middle East to the computer networks of foreign companies and groups seen as partisan to the conflict [Adams 2001].

³² Given the widespread use of automated attack tools, attacks against Internet-connected systems have become so commonplace that counts of the number of incidents reported provide increasingly less information with regard to assessing the scope and impact of attacks. An incident as reported in the figure may involve one site or hundreds (or even thousands) of sites. Also, some incidents may involve ongoing activity for long periods of time. Therefore, as of 2004, CERT will no longer publish the number of incidents reported [www.cert.org].

³³ We have compiled the figure from numbers from the Computer Emergency Response Team (CERT), a federally funded research and development center in Pittsburgh operated by Carnegie Mellon University [www.cert.org].

it reality it is not). Such incidents cause network administrators to be called in the middle of the night to check on systems. This causes a drain on both financial and human resources.

Historically, governments have not had a strong interest in addressing cyber sabotage and denial-of-service attacks because they were viewed as a commercial problem³⁴. This view has now changed. The governments of Canada and the U.S. have realized that the Internet is a national critical infrastructure that needs protection.

Protection of the Backbone: The Internet is largely immune from random failure of individual components. Despite frequent router problems, global network outages are rarely experienced or, despite the temporary unavailability of many web pages, our ability to surf and locate information on the web is relatively unaffected. However, the error tolerance comes at the expense of attack survivability [Albert Et. al 2000]. The topological weaknesses of the current communication networks, rooted in their inhomogeneous connectivity distribution, seriously reduce their attack survivability. The internet as an infrastructure is highly susceptible to targeted attacks on components critical to its connectivity.

Other issues of importance when discussing cyber protection are the increased use of wireless communication (also for PSS) and the increased number of identity thefts. The U.S. Federal Trade Commission received more than 200,000 identity theft complaints in 2003, or 42% of all complaints received³⁵ [FTC 2004]. The simplicity of stealing and using other people's identities makes it easier for terrorists and non-nationals to operate.

IS technologies can assist in many with these challenges. For instance, Survivable Network Systems is an emerging research field where IS technologies play an important role. IS tools can help ensure that networks of essential services are robust enough to survive intrusions by repeatedly testing or validating communication nodes, recognizing new vulnerabilities or intrusions, and recovering from an intrusion without any disruption to service provision [Ellison et al 1999].

P5: Smart Assistants and Communicators for Field Operators

The catastrophe following the seaquake last December showed the importance of efficient and targeted communication. Three technologies that played positive roles and contributed to the response efforts were ham radio, Short Messages Systems (SMS) and Internet blogs. Ham radio were operated in a number of environments as it power requirements are as simple as a car battery. It is easily transported and is resistant to breakdowns that are characteristic of more technology dependent communication infrastructures. SMS enabled large groups of people to be reached quickly³⁶. Internet blogs were used to coordinate information and channel work.

³⁴ It is difficult to mandate network protection because more than 90% of the networks that make up the internet are owned and operated by the private sector. In addition, corporations affected are uncomfortable sharing corporate cyber-security information with the government and as the attacks aren't physically or tangibly severe, it is difficult to quantify economic losses. Since many cyber-attacks focus on previously unidentified software vulnerabilities, it is almost impossible to establish legal liability. Moreover, from the legal angle, there is no deep-pocket recovery compensation obtainable from a convicted lone hacker in countries such as China or the Philippines.

³⁵ Internet related fraud accounted for 55% of all fraud reports received in 2003 by the U.S. Federal Trade Commission, for a loss of almost \$200 million.

³⁶ Multimedia Messaging Service (MMS) is an evolution of SMS that allows users to send pictures. A noteworthy application of MMS already being brought to market is Orange UK's initiative to use photo messaging at the scene of accidents. This allows hospital crews to assess the extent of injuries and respond accordingly.

Communicating with first responders in the field is crucial to the successful management and control of any PSS incident. Current communication systems are typically sequential, with multiple users queuing to use a single voice or data channel. If there are multiple channels, the problem is then one of communicating necessary information from one channel to another and hence from one responder to another. IS technologies can help track, interpret and manage these communications with field personnel and also ensure that appropriate information is passed to the appropriate people³⁷.

Field workers generally don't have easy access to information they need. Mobile technology provides this, whether in the form of pre-synchronized data on a handheld device, or through access over a wireless link. However, there are two problems with this. The first is that tomorrow's field workers need more than information - they need intelligent decision support. The second is that such decision support becomes more important in situations where communication links are failing.

Tomorrow's field workers are expected to need instant assistance. A trend towards more complex field situations that is more difficult for field operators and first responders to deal with without support is emerging. This means that field workers need smart assistants, i.e. decision support tools with some intelligence. An ideal communication system would be able to deal with voice and data inputs as well as translate and understand key PSS concepts in the communication streams, allow for operation independent of the command and control centers, and ensure that key information is accessible and utilized efficiently in a practical, user-centered device.

Examples of decision support tools for field workers include procedures, diagnosis, digital briefing, common operating pictures and interactive maps. Field operators and first responders can be provided with very effective situational awareness. For instance, such tools can communicate with a command and control center and display chemical or biological events and their predicted spread, giving an immediate and projected hazard prediction.

First versions of decision support tools for field workers are likely to be variations of hardened and wireless PDAs using touch screen, voice commands or helmet mounted displays³⁸. These PDAs are likely to support a range of text, video, graphics and voice communication, including burst transmission communication techniques.

P6: Multi-Organization Interoperability

Different organizations may need to see the available information from a PSS incident in different ways, and possibly, for different purposes. In some cases, information may need to be packaged formally for processing within the receiving organization. The information may also be used to evaluate the current situation and make decisions about levels of future support by the receiving organization, or it may be used as view-only information so that the receiver can monitor the situation. Being able to provide appropriate information to other organizations, and request or receive the same from them, during the course of a PSS incident is a possible task for an intelligent system.

³⁷ A system that is able to deal with voice and data and translate and understand key PSS concepts in the communication streams would be able to operate independently of the command and control centers and ensure that key information is used the best.

³⁸ Currently being developed for military use.

Noreen Allegre, Director, Police Services Branch of the Policing Services Division for the Minister of Community Safety and Correctional Services of Ontario stated in an interview for this study that if there had been better technology for police departments to share information the Paul Bernardo crimes may not have been committed. A new system that is now in place enables the police departments to share information across jurisdictions. In addition, patrols on the street are now able to access information from numerous sources, facilitating their ability to analyze and evaluate operations without have to return to their desks.

However, it's not just the ability to share information across police jurisdictions that is needed. Raymond St. Jean, Manager of the RCMP Integration and Policy Section Mobile Services Directorate, Engineering and Infrastructure Branch, would like communication links to be facilitated between public safety groups regardless of organization, protocol or vendor of communication device.

P7: High-Value Inspection

Good models for inspection are models that have a low ratio of probes to findings. A typical Acceptance-Rejection Quality Control approach is often used in manufacturing, where costs of sampling are balanced with those of passing bad items. This approach used for PSS can be shown to lead to inspection of, for example, all airline passengers and all baggage. However, in classical quality control, the system being inspected is not expected to react to the inspection methods being used. In PSS, this is not the case. It is expected that people will attempt to use information about inspection protocols to lessen the probability of their being detected. It is therefore necessary to move towards models whose analysis requires stochastic simulation and intelligent software agents playing adversary roles. These solutions need to be cost and time effective for successful implementation. Technologies from emergent behavior and game theory can be used to better find higher value inspection schedules.

One of the challenges in the area of personnel inspection is to be able to automatically authorize a person presenting an I.D and confirm that the person presenting the card is in fact the authorized user of the card. This would save significant time of security personnel that are required to inspect each piece of I.D. separately.³⁹

P8: Perimeter Control

Technologies for perimeter security for critical infrastructure can include access control and fencing with central control units and sensors⁴⁰. IS technologies can support the development of intelligent, symmetrical monitoring systems for the detection, recognition, and identification of possible threats and then provide the means for a possible first response to any perimeter threats, from a voice challenge/warning to a weapons attack.

In urban areas, the most important aspect of an automated perimeter security system is its ability to filter out normal intrusions and alarm only when something unusual approaches. This can be achieved with the use of cameras, heat-sensors and IS technologies. The Intelligent System would be able to distinguish between innocent intruders, such as wildlife or the scheduled arrival of a commercial jet, and an illegal intrusion. This means that humans would not need to constantly watch the video

³⁹ As illustrated by Charles Stearn, an analyst for Booz, Allen, Hamilton, in an interview for this study, December 2004.

⁴⁰ Such as the Fiber Fence system being offered by Fiber Instrument Sales Inc of Oriskany, New York.

screens, the systems would analyze, and alert security officers if something suspicious enters the security zone⁴¹.

Larry Brown, Director, Legal Affairs with the Edison Electric Institute (EEl) based in Washington D.C., stated in an interview for this study that his industry could use input from the IS sector for cost effective tools to help monitor perimeter security, a task that becomes very repetitive and difficult to do for long stretches of time. A “smart camera” (that identifies whether a potential threat was just a deer or in fact an intruder with malicious intent to weaken the infrastructure) would be a helpful addition to their tool kit.⁴²

P9: Evacuation and Crowd Control

Activities in this area should encompass all four phases of the incident management framework of preparedness, response, recovery and mitigation due to the potentially large number of individuals involved and the dynamic and unpredictable nature of human behavior when confronted with certain stimuli in stressful situations. Tools such as GPS tracking systems of police officers would allow incident commanders to track their movements at all times. Thus, when an outbreak occurs, they would be able to see who is in the immediate area to respond and position backup support.

P10: Social Network Analysis

Social-network-analysis technologies and methodologies can be adopted to uncover and understand terrorist communication and social networks to help the intelligence community detect future attacks. From another angle, social-network-analysis technologies and methodologies can be applied to developing a better understanding of the agencies involved in PSS. The number of organizations typically involved in PSS and PSS incidents make it difficult to follow the plethora of interaction points, interconnectivities and roles and responsibilities that are necessary.

P11: Intelligent Maps

Geographic information systems (GIS) have already revolutionized our ability to respond to homeland threats. GIS is a computer-displayed mapping system showing layers of data. Using a GIS, an operator can display a map of, for example, the entire city of Vancouver. Clicking on the Coal Harbor area of the map brings up details of that part of the city.

Much of the data necessary to support GIS maps already exists in digital or computer form, but unfortunately is often in disparate locations, agencies and formats. For example, the water department has water line data, electrical utilities have electrical transmission data, provincial forestry service has mapped vegetation, data on slopes is available from national geological databases, and housing developments are included in local government data.

⁴¹ Furthermore, the location and identity of intruders could be immediately transmitted to hand-held computers used by security officers in the area.

⁴² As per discussion with Larry Brown, Director, Legal Affairs, Retail Energy Services, December 6, 2004.

In the process of creating consolidated GIS databases, it would be advantageous to consider how IS technologies could be used to create what might be called “Intelligent Maps”. These maps would contain information and reasoning abilities that a user needs to perform specific tasks and would deliver information to the user in the most appropriate format for the tasks to be completed. Such maps could become invaluable for emergency planners and command and control centers.

P12: Detection and Sensing

As the number of threats grows, information overload can hinder the ability of PSS professionals to analyze and sift through to determine legitimate threats. The evolution of detection and surveillance tools is giving “first responders affordable tools with higher and faster throughput, greater precision and sensitivity, more portability and more flexibility than traditional tools” [Leggiere 2004].

Detection networks or stand alone sensors can replace humans for more dangerous tasks and can also provide a higher level of accuracy in carrying out activities within all of the incident management framework phases, i.e., preparedness, response, recovery and mitigation. A large number of technologies already exist in this area. For example, radiological sensors are available for police cars on patrol. Mobile radiation detection systems that operate as a network over a fixed area analyze data from a multitude of detection tools such as the Matrix MRDS system created by Thermo Electron Corp., of Waltham, Massachusetts.

IS can be used during planning to determine where and when to locate these sensors for specific tasks and incidents. They can also be used to do the same with mobile sensors that might be available during an actual incident. When coupled with mobile autonomous robots, whether on air, ground or water vehicles, these sensors could be positioned by an incident commander with the help of an intelligent system to gather the most appropriate information needed to detect and identify potential hazards in the current incident environment.

P13: Understanding critical infrastructure interdependences and protection needs

Critical infrastructure systems such as water, energy, telecommunications, computer, and networked banking are becoming increasingly interdependent. Consequently, the vulnerability of these stratified networks has reached a worrisome level. For instance, the normal operation of water, telecommunications and banking systems is maintained only if there is a steady supply of electric energy. On the other hand, the generation and delivery of electric power cannot be ensured without the provision of fuel, water, and various telecommunications and computer services for data transfer and control purposes to the power plants and networks. These interdependencies are becoming stronger as the usage of the Internet and other computer networks becomes prevalent.

Furthermore, some of these networks have huge geographical reach. For instance, the electrical power systems have reached continental size - there are 500,000 miles of high-voltage power lines across North America [Economist 2003]. These networks are complex and vulnerable. For instance, in the animal food chain network, as cattle remains are being fed to chickens, chicken remains can be fed back to cattle. This increases the probability of spreading disease while making tracking difficult. As another example, on August 14, 2003, the largest power blackout in North American history affected eight U.S. States and the Province of Ontario, leaving up to 50 million people

with no electricity [NRC-USDE 2004]⁴³. The ripple effects of this incident were widespread and affected the operation of many of Canada's critical infrastructures.

From the workshop and telephone discussions conducted for the study, it was revealed that the dependencies between critical infrastructures (CIs) as identified by PSEPC are not well understood. The full consequences of how challenges with or stoppage of supply from one CI could affect other CIs are not fully grasped. For example, Jane Pearce, Chief, Financial Crimes, Domestic Division, Financial Sector Policy Branch for Finance Canada, stated that the finance sector was highly dependent on both a supply of telecommunications services and hydro/electrical services. In addition, human resources that are essential for the smooth operations of the financial sector could be negatively impacted by a major flu pandemic. The scenarios that could be run considering only two or three sectors and how they might affect financial services is nearly endless.

Much of Canada's critical infrastructure is in densely populated areas, so if the country is attacked, average citizens, not uniformed military personnel, will be the most likely casualties. Police, firefighters, and emergency medical technicians will be the first on the scene of any attack; they will have to operate largely on their own for at least the first 12 to 24 hours. Yet we believe the average police and fire departments are not equipped for such events. For instance, police departments in cities across the country do not have the protective gear to safely secure a site following a WMD attack. And most emergency medical technicians lack the tools to determine which chemical or biological agent may have been used⁴⁴. This has impact on the probability of events propagating farther through the infrastructure dependency network.

⁴³ January 5-10, 1998, an ice storm knocked down a sizable segment of the electric transmission grid of Canada and the North Eastern region of the United States. The restoration of the Canadian network took months and cost the taxpayers several billion dollars. In France on December 17 and 26, 1999, two consecutive waves of windstorms left millions of people without electricity for several days (ABC News, 1999).

⁴⁴ There may also not be a full understanding of these needs. For instance, in fiscal year 2005, the U.S. Congress will give the Pentagon \$7.6 billion to improve security at military bases. Meanwhile, the Department of Homeland Security will receive just \$2.6 billion to protect all the vital systems throughout the country that sustain a modern society.

Intelligent Systems for PSS

The last ten years have seen the development of the technologies for providing necessary tools for the challenges of PSS. The reasons include:

1. **Increased computational power:** Computers have become more powerful and more widespread. The new breed of techniques in Intelligent Systems has largely been driven by experimentations, which could not have happened without this development. The computational power is now available to solve problems that could only be studied theoretically in the past.
2. **Increased connectivity:** Better integration between applications and the simple fact that everyone suddenly is on a network with everyone else have created both an availability of data, information and knowledge, and a pressure to provide reasoning power to leverage on this.
3. **Increased data availability:** New technologies, including wireless devices, Geographical Information and Positioning Systems, satellites, and cellular phones, collect unprecedented amounts of data.
4. **Emergence of new reasoning technologies:** A large body of research and development in Intelligent Systems has contributed strongly to bringing new opportunities for providing good tools for PSS.
5. **Confluence of technologies:** We see a confluence of several technologies that will help us develop the necessary tools for PSS. This includes work in Optimization, Operations Research, Artificial Intelligence, simulation, human-computer interaction and emergent systems⁴⁵.

It is likely that advances in Intelligent Systems technologies will transform the management of PSS from interagency communications, to use of decision support systems, simulation and analysis tools, and digital training environments. Intelligent Systems has the potential to enable us to plan for, manage and recover from incidents more efficiently than before, and is thus likely to enhance elements of decision-making in PSS.

For the sake of manageability, we will in this document define Intelligent Systems broadly, as a collection of technologies and approaches to problems solving. The table below lists a set of Intelligent Systems R&D and technology areas. The selections are broken down into two lists. The first one is a list of some Intelligent Systems application areas we believe are applicable for PSS. The second is a list of Intelligent Systems technologies we believe are applicable for PSS.

D	IS Application Areas Applicable for PSS
D1	Knowledge Discovery and Data Mining
D2	Knowledge Based Systems / Expert Systems
D3	Operations Intelligence
D4	Intelligent Simulation, Training and Tutoring

⁴⁵ For instance, a substantial body of development in Intelligent Systems has contributed enormously to bringing the state of the art in Operations Research forward and the gaming industry has made new interactive training methods possible.

Intelligent Systems for Public Safety and Security

D	IS Application Areas Applicable for PSS
D5	Machine Learning and Adaptive Systems
D6	Intelligent Human Computer Interaction
D7	Computer Vision
D8	Speech Recognition
D9	Robotics and Autonomous Systems
D10	Natural Language Processing and Generation
D11	Ambient Intelligence and Wearables

T	IS Technologies Applicable for PSS
T1	Deductive Reasoning
T2	Constraint Reasoning, Search, Heuristics
T3	Reasoning under Uncertainty, including Fuzzy Logic
T4	Case Based Reasoning
T5	Multi-Agent Systems
T6	Artificial Life, Swarms and Emergent Behavior
T7	Evolutionary Problem Solving and Genetic Algorithms
T8	Neural Networks
T9	Pattern Recognition
T10	Architectures
T11	Knowledge discovery and knowledge management
T12	Knowledge elicitation, representation, and modeling
T13	Game Theory
T14	Nanotechnology

The technology list (“T”-list) provides the most general starting point to discuss the potential applicability of IS for PSS. The list is however also significantly harder to explain to people not initiated in the field of IS. If discussions are based around this list, there is a possibility that the discussion becomes embedded in a technological discussion that would be difficult for non-experts in the field to follow.

The application area list (the “D” list, where the “D” stands for “Domain”) offers an alternative. The list acts as the departure point for the discussions, even though the potential for the underlying technologies greatly exceed those on the list. This list is to provide examples, but one’s imagination should not be limited to the scope included here.

D1: Analytics: Knowledge Discovery and Data Mining

Extracting relevant information from structured and unstructured data is crucial for the decision-making process. Examples include banks to detect credit card fraud, telephone companies to spot unauthorized use of the phone system, and supermarket chains to identify purchasing patterns.

Data mining, also known as knowledge-discovery in databases (KDD), is the practice of automatically looking for ways to discover patterns, structure, or associations in large bodies of data. Although it is usually used in relation to analysis of data, data mining is an umbrella term and is used with varied meaning in a wide range of contexts. It is a non-trivial extraction of implicit, previously unknown, and potentially useful information from data [Frawley et Al 1992]. To do this, data mining uses computational techniques from statistics and pattern recognition.

Data mining and pattern recognition have numerous applications in PSS⁴⁶. Data mining is often viewed as a potential means to identify suspicious activities, such as money transfers and communications, and to identify and track individuals, such as through travel and immigration records. Embedded data mining modules could also be crucial for making sense of data that is flowing through command and control centers. In addition, visual data mining techniques such as association rules and multidimensional-information visualization can help identify criminal relationships⁴⁷.

Pattern recognition techniques can be used to detect early warnings for outbreak of infectious diseases, for instance by monitoring Internet based news sources⁴⁸. Pattern recognition techniques are also used to recognize faces, fingerprints and irises, and also recognize people by the way they talk. In the area of PSS, biometrics is one area of pattern recognition that could be used for perimeter control and border security.

In an interview for this study, Steve Dische, Homeland Security and Counter Terrorism Specialist at the National Security Division of the Pacific Northwest National Laboratory, described STARLIGHT as a current example: STARLIGHT is a data mining tool designed for the US Army and more recently adopted in the US for use in homeland security. Once parameters containing key word data on how a particular infrastructure might be viewed throughout the world in open source media are defined, STARLIGHT then searches the sources for those keywords and patterns in how the information is presented. Upon implementation, several domestic US organizations were discovered as being talked about in ways that were not known previously. Those organizations were then able to respond appropriately.

D2: Knowledge Based Systems / Expert Systems

Digging up data, storing it and displaying it are worthwhile. However, we usually need more than data. We need decisions. To make decisions, we need knowledge.

The term data describes specific instances and events, while knowledge describes abstract classes and each class typically covers many instances [Wiederhold 1986]. Data may be gathered automatically or clerically, while experts are needed to gather and formalize knowledge. A knowledge base is a collection of knowledge. A Knowledge Based System (KBS) is a system that in addition to its represented knowledge is able to reason over this knowledge. A Knowledge Based System reasons based on rules and experiences derived from human experts aided by an inference engine that outputs guidance about operating conditions of a process or system.

⁴⁶ Data mining is emerging as one of the key features of many homeland security initiatives in the US. Two initiatives that have attracted significant attention include the now-discontinued Terrorism Information Awareness (TIA) project 13 conducted by the Defense Advanced Research Projects Agency (DARPA), and the Computer-Assisted Passenger Prescreening System II (CAPPS II) being developed by the Transportation Security Administration (TSA).

⁴⁷ Companies in this field include Attensity, InferX, COPLINK. COPLINK in particular has been used to discover links from various different data sources by law enforcement officials throughout North America.

⁴⁸ Such an application has been developed by a Montreal-based company, with funding from Ted Turner and assistance from the United Nations.

Expertise is deep knowledge of a certain field or problem. An Expert System should thus be a Knowledge Based System with specialization; in reality they are interchangeable terminologies.

Mycin, one of the first commercial Expert Systems, was already in business use 1974 [MIT, Applications of AI, 2001]. Mycin was a medical diagnosis tool. Given information concerning a patient's symptoms and test results, Mycin attempted to identify the cause of the patient's infection and suggested treatments. It performed better than medical students or practicing doctors, provided its limitations were observed.

Expert Systems have been developed for a variety of reasons, including: the archiving of rare skills, preserving the knowledge of retiring personnel, and to aggregate all of the available knowledge in a specific domain from several experts, (when no single expert has complete knowledge of that domain). The Expert System can train new employees or eliminate large amounts of the monotonous work humans do, thereby saving the expert's time for situations requiring his or her expertise.

Expertise to go around is not always available at the right place and the right time. The primary goal of expert systems is to make expertise available to decision makers and technicians who need answers quickly. Computers loaded with in-depth knowledge of specific subjects can bring decades' worth of knowledge to a problem.

These knowledge-based applications have enhanced productivity in business, science, engineering, and the military.

As an example, Dr. Liz Rohonczy, Containment and Safety Services Manager with the Canadian Food Inspection Agency, works in an environment characterized by disparate systems and highly specialized personnel. She emphasized in discussions with us the importance of capturing the expertise of subject matter experts in industries that face scarce human resources, mobile workforces (due to promotion and relocation) and an aging society. An expert system may be one of the ways to capture such information and provide continuity between personnel changes in highly specialized fields.

Expert Systems may also provide first responders at emergency sites with wireless diagnostic and surveillance tools to diagnose, to report and to communicate threats and countermeasures in real time. For instance, responders may carry computer-based personal assistants containing expert systems based decision support that can assist in prescribing medications in case of chemical or biological releases.

Systems that use these technologies, would also model established processes and procedures. For instance, during major incidents the requirements to follow local, provincial, federal and possibly international procedures during the course of the incident, especially as the nature or extent of the incident becomes more obvious, can become very complicated. A decision support tool that is capable of filtering the inflow of data, reducing complexity through reasoning and visualizing, has knowledge of these types of incidents, has knowledge of processes and procedures and the requirements to notify or involve various levels of the PSS infrastructure, could be an effective adjunct for incident commanders.

D3: Operations Intelligence

Expertise and knowledge can be embedded in computer systems in many different ways. Expert Systems subscribe to one approach, which is that expertise involves

logical thinking, and can be modeled by compiling lists of logical propositions and performing logical transformations upon them. Mechanized deductive rules are a common way of realizing this, hence they are also known as Rule Based Systems.

Complexity comes in several disguises. First, it comes from the sheer volume of data that tomorrow's commanders will be faced with. Secondly, it comes from the combinatorial nature of decisions, where the factors a decision is based on may combine in exponential ways. Tomorrow's command centers need help in managing both of these types of complexities.

Rule Based Systems are not a useful technology if the problems we are facing are combinatorial in some sense⁴⁹. Such systems are primarily used for representing and executing knowledge and expertise in environments that are structured. However, there are many problems that are inherently too complex and dynamic for this kind of reasoning. These are problems with combinatorial complexity, where the number of possibilities combines exponentially. Examples of such problems includes planning, allocation of resources to tasks, logistics, configuration and scheduling. The two fields of Operations Research (OR) and Artificial intelligence (AI) use different approaches to explore solutions in this area.

The last five to ten years have seen a confluence of technologies from the fields of Artificial Intelligence and Operations Research⁵⁰. The resulting work is often referred to as Operations Intelligence. Operations Intelligence provides a new generation of tools that better exploit the huge amount of data now becoming available during operations, and that profit from the use of novel innovative methods for managing complexity.

Operations Intelligence can be of significant assistance for PSS. For instance, preparedness often involves optimization planning for logistics, evacuation planning, routing, scheduling and depot locations. One example is *resource allocation*; the process of sourcing and scheduling resources, personnel (keep track of hours worked, location, job assigned), equipment (what agency has what, location of equipment), and support supplies (food for volunteers, shelter for out of town responders, etc). These tools could be used for risk management and creating awareness of interdependencies during preparedness, managing response and recovery, developing mitigation strategies and to identify and assess critical infrastructure linkages.

Operations Intelligence has made it possible to assist command and control centers managing the complexities of rapid decisions support in complex and dynamic environments *during* operations. This includes rapid rescheduling, dispatching and reallocation of resources when things don't follow plans. Examples include equipment breakdowns, sudden meteorological changes and additional follow-on incidents unfolding.

D4: Intelligent Simulation, Training and Tutoring

Emergency Management and First Response organizations often use "tabletop" exercises to practice elements of their emergency operations plans or incident command systems. Such exercises are useful for training and evaluating response, but they most often lack significant analysis into the broad spectrum of factors that influence preparedness. Computer-based simulations let students learn and experience the

⁴⁹ 'I think the next century will be the century of complexity.' Stephen Hawking.

⁵⁰ Notably optimization, graph theory, search, constraint programming and modern heuristics.

effects of different actions in a variety of situations. Electronic training simulations were pioneered by the aviation industry and the military and are being adopted by more and more businesses to help trainees learn diverse subjects such as equipment operations and maintenance, decision making during events and analytical skills.

Much Information Technology and IS research is useful for the gaming and simulation technologies, including work on software agents, emergent behavior and swarms, intelligent human-computer interaction, haptic interfaces, knowledge representation, representations of physical environments, and virtual reality.

Intelligent Simulation: Applications provide advanced methods to create better and more responsive simulation models, primarily for training and decision support purposes.

Intelligent Tutoring: Broadly defined, an intelligent tutoring system is educational software containing an artificial intelligence component. Like training simulations, Intelligent Tutoring Systems (ITS) enable participants to practice their skills by carrying out tasks within highly interactive learning environments. However, ITS goes beyond training simulations by answering user questions and providing individualized guidance. Unlike other computer-based training technologies, ITS systems assess each learner's actions within these interactive environments and develop a model of their knowledge, skills, and expertise. Based on the learner model, the software can make inferences about strengths and weaknesses, and can suggest additional knowledge area development for the student.⁵¹ ITS tailor instructional strategies, in terms of both the content and style, and provide explanations, hints, examples, demonstrations, and practice problems as needed. Recent trends have seen tutoring strategies moving away from fact based tutoring towards tutoring of problem solving strategies and the analysis of these strategies [Self, 1988]. As a result, the emergence of other learning environments, such as those that allow for experimentation and simulation and an increased range of interaction, is happening.

Electronic Games: An increasingly important source for the confluence of these technologies is the strong growth of the gaming industry. Videogames can be excellent training tools for command and control decision makers as well as field workers in PSS, and can be a powerful way to instill real-world skills⁵². The gaming sector has come up with some remarkable developments in simulation graphics while reducing development and production costs. The collateral impact of the technological developments in this field will continue as will the trend towards incorporating these innovations into training systems, delivering increasingly realistic and technologically advanced experiences.

Virtual Reality (VR): Most virtual reality environments (environments that are simulated by a computer), are primarily visual experiences, displayed either on a computer screen or through special stereoscopic goggles. Some simulations include additional sensory information, such as sound through speakers. Users can often interactively manipulate a VR environment, either through standard input devices like a keyboard, or through specially designed devices. The simulated environment can be similar to the real world—for example, in simulations for pilot or combat training—or it can differ

⁵¹ Early Intelligent Tutoring Systems incorporated an expert system, and a number of representational models were explored, including *if-then* rules, *if-then* rules with uncertainty measures, *semantic networks*, and *frames*.

⁵² The U.S. Marine Corps has used the commercial electronic game "Doom" to teach battlefield tactics, and a recent survey revealed that doctors who play videogames made 37 percent fewer mistakes during laparoscopic surgery [James 2004]. Simulators used in the Swedish defense training programs will be powered by technologies the gaming company Digital Illusions used to develop their game "Battlefield 2". The Serious Games Initiative is focused on uses for games in exploring management and leadership challenges facing the public sector [Serious Games 2004].

significantly from reality, as in VR games⁵³. Lately, the gaming industry and the Artificial Intelligence field have started to recognize each other. In 2005, the first conference of Artificial Intelligence and Interactive Digital Entertainment [Aide 2005] will take place.

It is clear that simulation systems and intelligent tutoring systems may have important roles to play in advanced training and preparedness in PSS. One example is medical training for first responders helping people subjected to chemical agents when accessing specific information is time critical. Another example is that responders and commanders can practice scenario exercises in simulated situations with chemical and biological agents that are too dangerous to use otherwise.

Supporting training and exercises with intelligent simulation systems are likely to be cost effective ways of allowing responders and commanders to practice the skills and communications they will need to deal with during PSS incidents. Such systems can provide consistent skills and techniques to all first responders. The information is available in a manner that does not require the first responders to leave their duty station (for instance medical personnel), as is frequently the case today. This may increase the amount of work they get done. Also, medical personnel will not depend on the initiative of local commanders to incorporate medical readiness training into their programs. A simulation model (virtual reality or common user interface) can provide a high degree of behavioral fidelity. This is the 'feel' that is critical to some procedures, like the ones the medical community is involved in.

As an example, during an interview for this study, Charlotte Rednar, a sanitary engineer with the Rhode Island Department of Health, stated that a system that is able to model and simulate how different biological agents interact with different bodies of water would be helpful to her department. Different biological agents interact much differently with different bodies of water depending on pH and many other factors. Being able to run accurate "what if" scenarios with different agents in different bodies of water would help the department in their preparedness, mitigation and response planning.

D5: Machine Learning and Adaptive Systems

It is difficult to encode all the knowledge that a system may need. It is also difficult to keep complex system knowledge up-to-date. Machine learning research focuses on how software systems can augment or refine their own knowledge to improve their performance.

Just as people use different learning techniques, machine-learning systems use a wide range of approaches⁵⁴. Some of these are supervised, in that they presume that the learner will have access to the correct answers; others are unsupervised, requiring the learner to proceed without benefit of feedback.

⁵³ In practice, it is very difficult to create a convincing virtual reality experience, due largely to technical limitations on processing power and image resolution. This type of technology is not widely available because of barriers. The most significant barrier is the requirement for high performance computers. Today there is a trade off between visual fidelity and the ability of the user to interact with the system. Thus, visual fidelity must be sacrificed so that a particular portion of the body has all its normal properties. There is also the issue of cost. Although a large amount of this technology exists, it is currently expensive.

⁵⁴ Learning is a rich and critical area with many techniques and approaches, including evolutionary computation, artificial life, concept learning, learning decision trees, probabilistic relational models, artificial neural networks, Bayesian learning, instance-based learning, genetic algorithms, and combined inductive and analytical learning. Hybrid approaches that integrate multiple learning techniques with reasoning and knowledge representations to synergistically improve both knowledge and learning are of interest.

Systems that have the ability to adapt to changing environments and learn beyond what is “programmed” into them are also called adaptive systems. These systems undergo changes, possibly random mutations and have the potential for self-organization.

Inductive learning systems learn by analyzing examples to identify correlations between inputs and outputs. For example, neural network models process inputs according to networks of idealized neurons, and learn by algorithms that adjust the weights of neural connections based on correlations between inputs and outputs in training examples. A neural network system to recognize faces might be trained on a digitized set of photographs of faces (inputs) and the associated identities (outputs), to learn which facial features are correlated with different individuals.

Software systems for PSS can benefit in substantial ways from machine learning techniques. For example, decision support systems that are regularly used in training exercises may learn that housing and blankets are more important during winter than summer. Machine learning can also be embedded in Personalized Assistants for first responders, where the system can learn to adapt to the specific needs of its owner.

Brian Scott, a Captain in the Information Warfare Aggressor Squadron of the Washington State National Guard interviewed for the study, stated that a system that is able to look for thresholds and attempted access to certain types of files on his systems would be most welcome. Furthermore, patch compliance programs and self-auditing systems would be useful IS tools to help with effectiveness and efficiency.

D6: Intelligent Human-Computer Interaction

An important example of confluence of technologies is the merging of reasoning technologies with radically new human-computer interfaces. Intelligent human-computer interaction (HCI) will provide intelligent support to the human user interacting with any PSS management support tools.

Intelligent user interfaces (IUI) are human-machine interfaces that aim to improve the efficiency, effectiveness, and naturalness of human-machine interaction (intelligent human-computer interaction, or HCI) by representing, reasoning, and acting on models of the user, domain, task, discourse, and media (e.g., graphics, natural language, gesture). Intelligent user interfaces are multifaceted, in purpose and nature, and include capabilities for multimedia input analysis, multimedia presentation generation, model-based interfaces, agent-based interfaces, and the use of user, discourse and task models to personalize and enhance interaction. Such an intelligent interface might anticipate the information required for a particular task that the user is performing and provide the user with only the necessary information in the most appropriate manner, perhaps modified by known user preferences for receiving data of that sort. The goal would be to ensure that the user retains an overall situational awareness of the incident progression, while at the same time having access to the detailed information required to solve a particular problem or perform a specific task in the most efficient and effective manner. Intelligent displays based on the information available at any particular time thus would filter, order or highlight that information to allow it to be used most effectively by the particular responder.

D8: Speech Recognition

In the 1990s, computer speech recognition reached a practical level for limited purposes. Thus, United Airlines has replaced its keyboard tree for flight information by a system

using speech recognition of flight numbers and city names. Telus customer service is now routed using a speech recognition system. Although the public has not generally accepted these systems as a replacement for more traditional input mechanisms, the technology has proven to be effective and practical.

D9: Robotics and Autonomous Systems

AI technology is being used in autonomous agents that independently monitor their surroundings, make decisions and act to achieve their goals without human intervention. For example, in space exploration, the lag times for communications between earth and probes make it essential for robotic space probes to be able to perform their own decision-making. Depending on the relative locations of Earth and Mars, one-way communication can take over 20 minutes. In a 1999 experiment, an AI system was given primary control of a spacecraft, NASA's Deep Space 1, 60,000,000 miles from earth, as a step towards autonomous robotic exploration of space [Nasa Rax 1 2004].

Methods from autonomous systems also promise to provide important technologies to aid humans. For example, in a 1996 experiment called "No Hands Across America," the RALPH system, a vision-based adaptive system to learn road features, was used to drive a vehicle for 98 percent of a trip from Washington, D.C., to San Diego, maintaining an average speed of 63 mph in daytime, dusk and night driving conditions [Pomerleau and Jochem, 1996]. Such systems could be used not only for autonomous vehicles, but also for safety systems to warn drivers if their vehicles deviate from a safe path.

Scientists have created models of robots that have legs, can gallop, navigate obstacles, and even swim [McGill University]. Autonomous robots have been used in the PSS context, particularly in situations where it is too risky for human responders to carry out tasks. Examples of such cases include hazard materials spill investigation and cleanup, and bomb disposal.

For PSS, robotics is of primary interest in perimeter control, surveillance and field operations. Examples include remote operations in contaminated areas.

D10: Natural Language Processing and Generation

Achieving natural interactions between humans and machines requires machines to understand and generate language. Likewise, understanding human communication requires the understanding of how language is processed by people. The nature of human language raises many challenging issues for language processing systems: natural language is elliptic, leaving much unstated, and its meaning is context-dependent. Machine translation systems, though still far from replacing human translators for literature, can now generate useful translations⁵⁵. The shortage of qualified Arabic translators is one of the key shortcomings of the intelligence gathering community in the United States, and the ability for IS to contribute to this field is sorely needed.

⁵⁵ Some natural language processing approaches investigate algorithms for syntactic parsing, to determine the grammatical structure of textual passages; others take a cognitively-inspired view, studying the knowledge structures underlying human understanding and modeling the process by which they are applied, or even attempting to directly apply expectations from memory to the parsing process. Other systems apply statistical methods to tasks, such as information extraction from newspaper articles.

D11: Ambient Intelligence and Wearables

An ambient device is one that provides useful information in a non-intrusive, background fashion — so that we can sense the information, much like one senses the temperature, humidity, or fragrance of a room, while maintaining one's foreground focus on other things⁵⁶. Ambient Intelligence represents a vision of the future of people surrounded by electronic environments, sensitive and responsive to people. Ambient intelligence technologies are expected to combine concepts of ubiquitous computing and IS while putting humans in the centre of technological developments. The research on Ambient Intelligence brings together researchers across multiple disciplines: computer science, artificial intelligence, electronics and mechanical engineering, design, architecture, social sciences, software engineering, to name a few⁵⁷. The main issues include:

- *Ubiquitous computing*: Wired, wireless and ad-hoc networking, discovery mechanisms, software architectures, system integration and prototyping, portable devices.
- *Context Awareness*: Sensors, tracking and positioning, smart devices, wearable, models of context of use, software architectures for multi platform interfaces.
- *Intelligence*: Learning algorithms, user profiling, personalisation and adaptivity, recommenders, autonomous intelligence, agent based user interfaces.
- *Natural user-system interaction*: Ambient interfaces, multimodal interaction, innovative interaction styles and concepts.

This development may have important impacts on PSS. Systems for critical infrastructure could be linked to key responders' PDAs. The responders can know where everyone is and communicate where they are to others provide routes as to where to go and what to do as per the emergency situation, indicate who is not physically available (PDA off or on holiday), and indicate where the responding agencies should assemble if the EOC is not available due to emergency environment. Thus, it could be used for information sharing during response and recovery and risk management during preparedness, response and recovery phases or to coordinate information regarding threats and warnings. These intelligent devices thus provide tactical level support for issues ranging from medical information for analyzing symptoms (a lot of work going on in this area right now), floor plans and intelligence for incident/site commanders. They also act as a tool that identifies and analyses intelligence by source (i.e. CSIS vs. member of public).

⁵⁶ You can purchase a grapefruit-sized orb from Ambient Devices, which requires electric power but no overt connection to the Internet; instead, it takes advantage of existing long-range (SMS, 2.5G, pager network), and emerging short-range (Bluetooth, 802.11) wireless connectivity technology. Once having plugged the Ambient Orb into AC power, it proceeds to glow and/or throb silently, depending on which "channel" you've set it up to monitor; available (free) choices are stock market averages, weather, traffic alerts and Homeland Security Alert Status.

⁵⁷ The European Commission intends for the EU to achieve world leadership in Information Societies technologies within ten years. To that end, it has incorporated the Ambient Intelligence vision in its Sixth Framework Programme with a budget of € 3.625 billion.

Discussion and Conclusions

A phenomenal progress in information technologies and telecommunications has immersed us in an all-computing and all-communicating world. It seems marvelous; the question is how we can use it to the benefit of PSS.

Precarn arranged a small discussion workshop on how Intelligent Systems can assist the field of Public Safety and Security in Ottawa on January 20th. The workshop participants, both from the intelligent systems sector and the PSS sector, had read an early draft of this report in preparation for the workshop. For readability reasons, we chose to not describe the discussions and results from the workshop separately, but have embedded them into the document.

On the PSS side, we believe it is not necessary to extrapolate trends five or ten years into the future; we believe it is sufficient to state that we believe the sector will come under significant increased pressure. We will start this chapter, however, with discussing some trends in science and technology that may be of assistance for PSS sector.

We will then draw some basic conclusions before we list some general recommendations.

Trends in Science and Technology

We see several ways that Information Technology and Intelligent Systems can assist in meeting some pressing PSS challenges already today. However, what are the trends in the technology sector that can have impact on PSS not today, but in the future? What are the trends that are more likely to happen, and which of these will have impact on the PSS field? It is hard to predict, especially about the future⁵⁸. The future is more likely to unfold in non-linear fashion. In the current era of technological innovation, the range of possible outcomes is greater than ever.

When that is said, the list underneath is a non-sensational extrapolation of select trends in science and technology. Some of them may have a strong impact on public safety and security and thus are worthy of exploring briefly in this paper.

1: University research becomes more systems-oriented and multi-disciplinary

In the past, scientific methods and institutions have tended to emphasize the study of individual natural processes rather than systems, on analysis more than synthesis, and on understanding nature more than predicting its behavior. Science has generally studied well-defined, small scale, short-term problems, usually in a mono-disciplinary mode, rather than on long-term, large-scale or integrated problems.

However, many of the problems in PSS need a systemic and multi-disciplinary approach. Greater effort will be needed to understand integrated systems on multiple time and space scales. Inter-disciplinary is becoming increasingly important. Almost all of the new leading-edge fields in science, including genetics, brain research, and

⁵⁸ Technologists and inventors of a new technology are typically the worst ones to predict and anticipate the ultimate use to which their invention is put. Thomas Edison had a "top 10" list of recommended applications for his invention called the phonograph; recording of music was number 7 on the list [Basalla 1990].

nanotechnology, materials science, robotics and automation, require interdisciplinary R&D. Furthermore, the challenges of PSS demand it and given the importance of the tasks our societies will be faced with that warrant integration, such as PSS, the distinction between basic science, applied science and technology will continue to decrease.

2: Computers will be able to manage essential systems

R&D initiatives in computer applications will permit essential systems, such as transportation and food production, to be managed in a more efficient manner. The downside of such systems is that this creates a new level of vulnerability as we increase our reliance on technology.

3: Computers will become essential decision support tools

In addition to assisting humans with difficult proactive tasks, such as planning and scheduling, systems that are designed for interactivity and reactivity will be developed for managing complex tasks.

Interactivity: Tomorrow's decision support systems will be true "shared initiative systems"; i.e. the human and the system cooperate in solving difficult tasks⁵⁹. Computers and humans have complementary strengths; decision support systems that amplify the positive outcomes of their interaction ensure convergence to superior solutions. Examples include tools that facilitate the rapid re-allocation of resources in dynamic situations with many constraints.

Reactivity: Compared to human operators, tomorrow's decision support systems will be able to find better solutions faster to complex and chaotic situations⁶⁰.

In both cases, such systems will become important tools for crisis management, and will be used in command and control centers.

4: We will all play video games

Education, training and preparedness will become experiences fueled by the gaming industry and the IS field. Simulation, training and tutoring will be more effectively and efficiently conducted with applications and tools developed with the concepts of what we today think of as part of the entertainment industry: video games and gaming consoles.

5: Computer chips will be "everywhere"

Already, telephones, televisions, music players, PDAs, domestic appliances and cars are packed full of electronics⁶¹. In the developed world, our day-to-day contact with

⁵⁹ Computers and humans have complementary strengths, and decision support systems that amplify this ensure rapid convergence to solutions for difficult problems. Examples include rapid emergency reallocation of resources in unclear situations with many constraints.

⁶⁰ What is complex today is likely to become more complex in the future. For instance, it is harder to evacuate Vancouver's downtown when the population density has increased.

⁶¹ General computers will be a very small fraction of devices that computer chips can be found in. An indication is that Apple Corporation market their latest Macintosh computer as an entertainment unit, not as a personal computer

computer chips is growing to the point that even our pets are interacting with them (i.e., tracking systems).

Computer chips will create a plethora of new products. The development of new products continues, with each year seeing smaller, faster and more technologically advanced tools, gadgets and applications. Many products we rely on today wouldn't exist without the miniaturized modern computer chips. The possibilities for the future are unimaginable just as today's tools would have been in the early 1900's.

Computer chips will enhance existing products. Old products will be enhanced by computer chips, as with watches, music players and cars.

Computer chips will be "invisible". Computer chips will be embedded in everything from brains and hearts, to clothes and toys.

Computer chips really will be "everywhere". Known as ubiquitous computing, calm technology or the Evernet, the notion is that instead of people being slaves to the computer, computers will be enslaved to humans. Computers will be everywhere; miniaturization will put a microchip in every object, from beer bottles to buses. All the chips could continuously interact, some collecting and sharing data, others acting on it.

Raymond St. Jean, Manager of the RCMP Integration and Policy Section Mobile Services Directorate under the Engineering and Infrastructure Branch hopes that the time for the full PDA integration and wearable computers for officers on the street is not far off as the advantages it will provide to law enforcement are numerous.

6: Personalization will gradually become useful

Tomorrow's devices will learn the patterns of their users. From a user's point of view, it may seem that their devices become intuitive ---they will "learn," "recognize," and "know" what we want. In short, this will give us much more effective human-device interaction.

7: Devices will communicate

A phenomenal progress in information technologies and telecommunications has immersed us in an all-communicating world. Computers, telephones, televisions, domestic appliances and cars are packed full of electronics for the exchange of data and information. Products (with embedded computer chips) will become voice-activated, networked, video-enabled, and connected together over the internet, linking with each other and humans. Many products will have digital senses - speech, sight, smell, and hearing - enabling them to communicate with humans and other machines.

8: We will have idiot savant devices

An idiot savant is an intellectually disabled person who exhibits extraordinary ability in a highly specialized area. What is meant by an idiot savant device, is a device that is exceptionally smart at one or a few things. Neural networks and other forms of artificial intelligence will make computers smart at certain well-defined tasks, in many cases smarter than humans⁶². An example of a potential tool for PSS, is a hand-held device

⁶² We will not have achieved "artificial intelligence", but in certain areas "artificial idiot savant".

that field workers can be equipped with that operate as an intelligent assistant for certain things, such as a medical diagnosis advisor or a course of action analyst.

9: Computers will gradually be seen as extensions of human beings

There is a potential for computers to be designed to augment health, intelligence, learning, communications, and productivity.

10: Robots for household chores or companionship will become dexterous, sophisticated, and cheap

There are currently several robots for household chores⁶³ and companionship⁶⁴ on the market. Applications for the PSS sector could be the adaptation of these tools to special uses for certain operational PSS environments. These types of applications are already in use. For example, some U.S. hospitals currently use a 180-kg wheeled robot to ferry medications from the pharmacy to nursing stations⁶⁵.

11: Technology convergence will blur the conceptual boundaries between technologies

The conceptual and practical boundaries between technologies and the way they are used are breaking down. In the near future, more and more things people use will incorporate a range of technologies, seamlessly put together⁶⁶.

12: We're going from data overload to information overload

Over the last ten years, technologies like wireless devices, Enterprise Resource Planning (ERP) systems, sensor networks, digital surveillance camera and geographical positioning systems have created an enormous amount of data. A consequence for the PSS sector is a growing concern about:

1. *How to extract information from all this data.* We already see a strong focus from the Homeland Security Advanced Research Projects Agency (HSARPA) on this problem through their massive funding initiatives in intelligent sensor networks, data mining and analytics.
2. *How to transform the information to decisions.* When the problem with creating information from the data has been addressed, it will become apparent that information is not enough. Data overload has been transferred to information overload. Making informed decisions based on that information is often not easy and requires further analysis. Drawing the right conclusions in complex and dynamic

⁶³ For instance, the "Rhumba" autonomous vacuum cleaner.

⁶⁴ Such as Sony's AIBO and QRIO.

⁶⁵ The robot is called droid named TOBOR (which is "robot" backwards"), which is produced by California-based Pyxis Corp., TOBOR uses sonar and infrared beams to find its way around patients and staff, and calls for the elevator using a radio signal. TOBOR can be leased for US\$5 an hour, and thus frees up time and financial resources.

⁶⁶ A simple example is Apple Corporation's music player "iPod". Its success can be attributed to a large extent to the integration between the device, the personal computer, the Internet and online services.

environments is inherently difficult⁶⁷. In complex operations, decision support is thus more than providing operational information; it also entails assisting in the analysis and reasoning leading to the best set of decisions. For this, IS have provided a new breed of reasoning technologies. Computers will become a necessary tool to transfer information into decisions.

Overall Conclusions

1: PSS will meet increasing challenges⁶⁸.

Current climatic, sociological and geo-political trends make it plausible that the PSS sector in Canada will come under increasing pressure. The public, as well as the governments on municipal, provincial and federal levels will expect and ask for more from the sector. It is also not unlikely that Canada will be asked to participate in a multi-national disaster rapid response task force⁶⁹, even on a level much larger than the seaquake response in Southeast Asia.

2: Technology will increasingly be applied to meeting these challenges⁷⁰

As is frequently the case when decision makers confront complex and challenging problems, the science and technology community is being called upon to contribute to national goals, this time to ensure public safety and security in an environment of increasing complexity, vulnerability and asymmetric threats⁷¹. We believe that Information Technology and Intelligent Systems sectors will be asked to help.

We also believe that advancements in science and technology will be critical to public safety and security in the future. Improving intelligence analysis, cyber-security, border security, emergency response, coordination of field workers and stake holders, planning and preparation all will require the invention and deployment of new technologies, ranging from new software to make computer networks more secure to new standards to make emergency response communications equipment interoperable.

3: Intelligent Systems technologies will play an important part

In MIT's annual list of "10 emerging technologies that will change your world" in 2004, the majority are IS technologies or have elements of IS technologies, including automated universal translation, synthetic biology, Bayesian machine learning and power-grid control [10 Emerging 2004]. Of Profit Magazine's 20 "bold predictions for the next 20 years", nine incorporate IS technologies [Portsmouth 2002].

IS technologies will transform the way we live and work. They will deliver productivity gains in many existing industries, revolutionize the delivery of social services such as

⁶⁷ Many of these problems are known as being NP hard, which is a way of saying that the complexity of solving the problems grows exponentially with the size of the problem. Examples include resource allocation, scheduling, logistics, planning and chess.

⁶⁸ Polemic: We're in over our heads.

⁶⁹ Some European Union members agreed on January 10 to push for the creation of a U.N. rapid-reaction force for humanitarian disasters (after a public call from President Jacques Chirac), dubbed the "white helmets" in the past after the U.N.'s blue helmet peacekeeping forces.

⁷⁰ Polemic: Prey that somebody will invent something that makes the problems go away.

⁷¹ Some recent newspaper headlines read: "Technology That Will Save Billions From Starvation." "Failure to Use Science 'Letting Down World's Poor', Says UN." "Can nanotechnology help solve the world's energy problems?"

health care, and provide the basis for many new companies. It is without a doubt that they will have an important contribution to make to PSS.

4: Technology is a large part of the problem⁷²

As part of California's effort in the war on terror, state legislators last year proposed that trucks hauling hazardous materials be fitted with technologies that would allow authorities to seize control of hijacked vehicles--a law that supporters said should be passed "on an emergency basis." The bill, however, was voted down after critics contended that the very people it was supposed to stop could easily commandeer the communication signals used in the proposed system.

Ironic as it may, the more we rely on technology to manage our PSS challenges, the more we're in trouble. The most useful technology used during the initial response efforts for the Southeast Asian tsunami, were ham radios, cellular phones and weblogs.

5: There is enough commonality to keep cost down

A lack of commonality between the PSS incidents would make our work harder and costlier. The question is how generic systems we can make.

We believe that there is enough commonality between PSS incidents that some tools can be developed to be generic enough to enable them to be affordable. Natural, technological, and terrorist-induced disasters are analogous in many important ways before, during, and after impact. Each type of incident may require incident command organization, information technology, warnings, communications, evacuation, special needs populations, feeding and sheltering, volunteers, emotional counseling, and stability of lifelines. Thus, lessons can be drawn and applied among all three, including:

- A common approach to disaster management can be conceived for natural, technological, and terrorist-related disasters involving preparedness, detection, response, and recovery. Systems, such as FEMA's Incident Management System (IMS) illustrates that this can be done.
- In all types of disasters, communication is needed among policymakers, first responders, public health workers, public service officials, practitioners, and researchers so all groups can work together efficiently and successfully during emergency situations. The key here is to ensure that the stakeholders have access to the tools.
- An incident command structure is needed to effectively manage disaster situations. Also, robust network-based (peer to peer) organizations could be developed following a similar framework for a varying combinations of stakeholders and incidents.
- Extensive planning and preventive measures are needed for all disasters, but equally important is the ability to improvise solutions for unforeseen problems that inevitably develop. Each incident will have its unique factors, not only in its specific characteristics, but also as the incident unfolds.

⁷² Polemic: Technology is a bad idea.

- Most PSS incidents start of as local incidents, some progressing to be larger in scale either retaining local command leadership or command could be passed from local to provincial to national lead agencies. Thus, effective local response is essential for responding to natural, technological, and terrorist-induced disasters.

Recommendations

In the report, areas where IS technologies can be used to help the PSS field with meeting some of its increasing challenges are presented along with recommendations and areas for action.

This study has been mandated with giving recommendations, though without constraints on which type of recommendations. Some of these recommendations don't fall directly under PRECARN's current mandate. The challenges facing PSS are many and complex, today and the response as a nation is scattered and confused. There is a duty to raise the awareness of the situation and help wherever possible. It is hoped that PRECARN, and other readers of this report, take this as a challenge to influence where they can. The challenges need to be looked at with fresh eyes and creative minds.

1: Do a more thorough study than this

This report is a result of a very short study with few resources. The problem addressed in this report – how information technology and IS can assist the field of PSS – is very important and deserves a more thorough treatment. An more in-depth, independent, comprehensive and creative study should be done.

A recent study conducted for the federal Centers for Disease Control and Prevention based on interviews with 190 first responders from 83 organizations across the U.S. showed that the workers "felt they did not know what they needed to protect against, what protection was appropriate and where to look for it," according to the report [LaTourrette et al 2002, Jackson et al 2003, Jackson et al 2004] . We don't think this perspective is limited to first responders in the U.S., or that it is limited to first responders in general. We would like to see a thorough investigation into the needs in the PSS sector combined with a broader investigation of the potentiality of modern technologies to remedy these needs while expanding the awareness of all the stakeholders involved in PSS.

2: Create financial R&D incentives for PSS

Governments will increasingly look to universities, laboratories and advanced technology companies for help in meeting the increasing number of challenges in the PSS sector. The IT and IS sectors in Canada are not prepared for this. These sectors are currently unaware of PSS as a domain to advance R&D. The reason is simple; these sectors follow the money, and currently that leads them elsewhere.

Canada should create financial incentives to raise the awareness and focus research towards tackling the mounting challenges that PSS are facing. Canada should create a comprehensive funding program for addressing the PSS challenges through technological innovation. An example would be a joint PRECARN / PSEPC program.

This report shows many examples of areas where Canadian R&D can make a difference for Canadian PSS needs. Examples included promoting the wide use of synthetic

training and tutoring environments, and developing tools for first responders, such as PDA's with email, the internet, telephone, GPS and dynamic maps.

3: Create both “science for policy” and “policy for science” programs

Connecting science and technology with decision-making is challenging. The path from scientific discovery to societal benefit is neither certain nor straight.

The phrases “science for policy” and “policy for science” are sometimes used to distinguish the two-way connections between research and decision-making. The former focuses attention on producing knowledge and technologies useful for those responsible for making decisions; examples might include the development of reliable, low-cost vaccines against bio-terrorism, decision support systems for command and control centers, or detection systems for nuclear or biological weapons. The latter focuses on how the scientific enterprise itself is organized, supported, and evaluated, ultimately to produce useful knowledge and technologies.

We believe that the new reality surrounding public safety and security has important implications for both “policy for science” and “science for policy”. Our focus in this report is on “science for policy”. However, the participants in a “science for policy” program in the PSS sector needs to be backed up by a “policy for science” program.

4: Create incentives for interdisciplinary team-based research and development

The challenges faced by PSS call for systems-oriented and interdisciplinary R&D, applied research and development conducted in teams that have the common objective of addressing the problems they have been asked to solve. We therefore recommend finding creative solutions to get universities to unleash their considerable science potential on common goals that are important for our future.

A large constraint to this is that universities neither have the necessary sticks nor carrots to make that happen. The internal award structures in universities in general tend to not support industry collaboration, teamwork or applied and interdisciplinary research⁷³. As a partial mechanism for dealing with the need for interdisciplinary, universities often set up institutes, which are more often than not only loosely linked to the basic science departments' teaching and curricula⁷⁴. However, interdisciplinary science may make greater inroads with the collaboration of governmental laboratories, private contractors, and large non-profit organizations.

The loosely defined nature of Intelligent Systems has a positive influence as it is flexible and can work with other disciplines as it is emerging and maturing as a field. Other technologies that can integrate well with Intelligent Systems include nanotechnology, computational biology, artificial life, emergent behavior, emergent computation, operations research, swarm technologies, game theory, and haptic interfaces. Hence, we recommend to Precarn to apply a broad view and a broad definition of Intelligent Systems.

⁷³ Yes, officially they do; however, the reality in most universities is that university professors that follow that call get punished in the tenure committees.

⁷⁴ There clearly are exceptions to this situation, but as a rule the bulk of North American universities interdisciplinarity can be seen as aspiration or as empty claims rather than as reality.

5: Create a program for transferring defense technology to the civilian PSS sector

Paradoxically, the military probably became the twentieth century's dominant producer of new cultural forms. It has generated massive innovation that has affected almost every practice — from materials science, to command and control, to robotics and communications.

The military in both the United States and Canada have invested very large sums in technology, some of which is transferred over to the civilian sector. There are programs in place to bring technology developed for specific applications into the commercial marketplace⁷⁵. Some of the results could very well be applicable for the PSS sector. However, we believe that neither Canada nor the United States has a sophisticated approach to sharing technologies and lessons learned in the military sector for civilian homeland security needs [Carafano 2004]⁷⁶. This type of information sharing may require a technology clearinghouse to enable partners know what technologies are available for transfer. This would entail a method to set standards so that technologies are understandable, interoperable and transferable to start a military-to-PSS dialogue that could include elements of predictable technology “export” control requirements, and acquisition mechanisms such as joint development programs.

However, technology transfer from one cultural context to another is a striking way of bringing the values embedded in technologies to the forefront. Technology transfer from military to (civilian) PSS will meet unexpected hurdles. For instance, the military is a hierarchic organization with well-defined parts, while the PSS sector consists of multiple organizations with different cultures, employing civilians of all ages and expertise. Early results from the U.S. show that military training and tutoring systems are difficult to adapt for use in homeland security environments.

6: Ensure that technological solutions support peer-to-peer (P2P) based organizations

The network may be the next major form of organization⁷⁷ to come into its own to redefine societies⁷⁸. We believe emergency response organizations will move towards a distributed way of organization. A polemic is that command and control centers are a bad idea. The following analogy is applicable: when the internet saw an increased use of file sharing technologies to share music files, it did not take long for the music industry to shut down the early operations (for instance Napster). The reason was that the music distribution was server based and there was a small amount of servers servicing the music down-loaders. However, soon after the early networks were crippled, the internet saw the emergence of file sharing networks based on the peer-to-peer principle. Peer-to-peer is also known as “network centric” or “power to the edge”. These are networks that are much harder to incapacitate, as each node in the network operates on a peer level with any other node. Hence, there are no servers, or for the analogy, there are no command and control centers to shut down.

⁷⁵ The U.S. Department of Defense had revenue of nearly US\$10 million in 2003 from patents and royalties [Gonsalves 2004].

⁷⁶ There are programs in place to bring technology out to companies for commercialization. The U.S. Department of Defense had revenue of nearly US\$10 million in 2003 from patents and royalties [Gonsalves 2004].

⁷⁷ After tribes, hierarchies, and markets.

⁷⁸ Also in war, where the term netwar calls attention to the prospect that network-based conflict and crime will be major phenomena in the years ahead.

In anticipation of this development, we recommend that technology developments are ensured to support P2P based operations.

7: Facilitate communication

Some of the information technologies that various PSS organizations must access have become very expensive. Bandwidth cost and the ability to bring information systems together to better work together were thought to be of highest importance.

The ability to anonymously share information within both government and industry is a concern. While the United States has the Information Sharing Analysis Centres (ISAC), Canada has no such similar program that has industry involved to such a great extent. Centres, such as the ISACs, allow these corporations to reveal this information anonymously. The information is then spread out and helps the industry as a whole recover and respond better to that particular vulnerability. Canadian corporations are concerned that if they reveal a particular vulnerability it could adversely affect their reputation in the marketplace.

Parallel to the problem of getting industry to collaborate, government departments, for mostly political reasons, often have difficulty, or refuse, to share information. If they do decide to share, the variety of systems that are used at the municipal, provincial and national level as well as within the multitude of government departments and organizations hinder the development of a secure means for departments to talk to each other.

A concern that was repeated several times during this study was a feeling of potential poor coordination between organizations in general, and especially during emergencies. With all the organizations involved in a potential catastrophic disaster, there are many different groups that could function in a variety of roles and responsibilities. Ensuring that the responding agencies are coordinated at all levels is essential to a successful emergency management program. “Power to the edge” type thinking is not happening enough; there is too much reliance on people at the top.

8: Focus on “demand-pull” rather than “tech-push”.

R&D programs for the benefit of PSS should continue to be more “demand-pull” than “tech-push”. This will ensure that the technologies that are developed for and applied to PSS will be created from real needs and address real problems.

“Demand” is not well defined in non-market environments such as public safety and security. However, measuring the impact of certain events, and hence the positive impact of preparing for them or avoiding for them, can be used to drive policy. This may very well lead to policy decisions that are unexpected. For instance, the current focus on the consequences of terrorist attacks may be revised in the light that such attacks may have a lower probability and a lower death rate compared to natural hazards⁷⁹ or the potential of a large influenza epidemic. Terrorist attacks are very rare. So rare, in fact, that the odds of being the victim of one in an industrialized country are almost non-existent. And most attacks affect only a few people. The events of September 11 were a statistical anomaly. Even counting the toll they took, only 2,978 people in the US died

⁷⁹ This concern was also raised by one of the interviewees for this study, Larry Brown, Director, Legal Affairs, Retail Energy Services, December 6, 2004.

from terrorism in 2001. That same year, 157,400 Americans died of lung cancer, 42,116 in road accidents, and 3,454 from malnutrition.

9: Complement Other Programs

We propose that any technological R&D programs that would benefit the PSS sector should complement instead of follow other programs. An important example is the large research programs under DARPA and HSARPA in the U.S. HSARPA's first annual budget is approximately US\$1 billion, focusing on areas that include networked biological and chemical sensors, systems architectures for managing sensor networks, radiation and nuclear-threat detection systems, as well as decontamination systems.

10: Facilitate cross-border integration

Canada-U.S. cross-border integration could be improved for a wide range of issues such as security, logistics and movement of goods⁸⁰. For example, does Canada have the diversification needed so that if serious security threats necessitated the United States closing or highly restricting their borders Canada could continue operations internally without debilitating the economy or hindering the PSS of our citizens?

⁸⁰ It may be seen as ironic that today you can drive from the North Cape to Gibraltar without even noticing that you're crossing a international border, while driving from Vancouver to Seattle can be quite a hassle.

Appendix 1: The PSS Landscape in Canada

A successful resolution of most PSS incidents requires the management of a wide range of human and materiel resources. The unique components that exist in every emergency and the dynamic nature of PSS incidents dictate the need for a wide range of interagency collaboration at a number of levels.

Under the lead of the federal Ministry of Public Safety and Emergency Preparedness Canada (PSEPC), the stakeholders in PSS include (but are not limited to) the following: Public Safety and Emergency Preparedness Canada (PSEPC), National Resources Canada (NRCan), Industry Canada (IC), Finance Canada (FC), Health Canada (HC), Agriculture and Agri-Food Canada (AAFC), Canadian Food Inspection Agency (CFIA), Canada Border Services Agency (CBSA), Environment Canada (EC), Transport Canada (TC), National Defence (DND), Treasury Board Secretariat (TBS), Canadian Security Intelligence Service (CSIS), Foreign Affairs Canada (FAC), RCMP, Privy Council Office (PCO), provincial/territorial Emergency Measures Organisations (EMO), provincial / territorial government agencies (including hospitals), municipal government agencies (including first responder organizations), non-government organizations (such as the Canadian Red Cross and the Salvation Army, etc), community organizations, private industry (critical infrastructure), and members of the public.

The breadth of this list illustrates the amount of collaboration between multiple agencies that is necessary to tackle the challenges of PSS in Canada. No entity has the resources or the capability to “go it alone”. This is strongly reflected in the overlying characteristics of PSS in Canada.

Characteristics of PSS in Canada

The overlying characteristics of PSS in Canada can be characterized in the following way⁸¹:

1. Level of operation:

As with military operations, activities are carried out across three levels of operation: strategic, operational and tactical. Each level of operation will have different needs and requirements. Key considerations include that many activities are unique and are not consistent across all three levels; the effects of an incident can cause conflicting priorities across the three levels and that the stakeholders involved may be different across the three levels.

2. Interagency collaboration:

The necessity to share resources and the broad range of stakeholders affected in emergencies warrants the need for multiple agencies to collaborate in all areas of emergency management.

⁸¹ The list is meant to highlight key areas to provide an understanding of the field.

3. All emergencies start as local emergencies:

Incidents start off small and local and thus the framework of response starts with the individual and proceeds to include municipal, then provincial and then federal support. The pace of an incident's intensity and the scope of its impact will vary in each situation and set the requirements for the nature of support that will be required.

4. National Defence in a support role:

The Department of National Defence (DND) assets support the first responders in PSS incidents as requested through established channels as per the National Defence Act. In a few circumstances, for example, under a request for armed assistance, incident command may be passed to DND, but it would be for a limited period of time and to complete a specific task.

5. Multiple Emergency Operations Centres (EOCs) (for command and control):

There are numerous EOCs within Canada. For example: PSEPC's Government Emergency Operation Centre (GEOC), the RCMP's National Operation Centre (NOC), DND's National Defence Command Centre (NDCC), various Departmental Operation Centres (DOC) and Ministry Operation Centres (MOC), provincial EOCs (Nova Scotia's Joint Emergency Operations Centre (JEOC), BC's Emergency Coordination Centre (ECC)), municipal EOCs, first responder agency Incident Command are just a few of the many EOCs that must be coordinated.

6. Communications:

Communication systems consisting of fax, phone, paper and person-to-person liaison provide less of a challenge to information management than the question of compatibility across various IT systems and platforms used within the collaborating agencies. Email has become the only "high tech" tool used for collecting and disseminating information in most command centres in Canada as system-to-system interoperability poses more challenges to communication and information sharing.

7. Composition and structure of agencies is not consistent:

Provincial/territorial EMOs do not follow a consistent organization naming convention (ie Emergencies Measures Alberta, Emergency Measures Organisation Ontario, Nunavut Emergency Management, etc). In addition, provincial and municipal government agencies responsibilities may vary from province to province, with the organizational charts providing a challenge for understanding roles and responsibilities in emergency management

8. Levels of activation:

Different levels of an emergency require different activities. For example, Health Canada has the following activation procedure which outlines activities of the department:

- *Level 1 – EOC is on standby (general operation level with no emergency)*
- *Level 2 - EOC begins monitoring a situation with a limited staff.*

- *Level 3 - Health Canada's Emergency Response Plan is activated.*
- *Level 4 - EOC staff is expanded to provide up to 24/7 support.*

This procedure will be activated internally to Health Canada. Other activation procedures can be occurring in tandem in other government departments as well as under the federal system, a provincial/territorial system or a municipal system of activation.

9. Logistics:

The logistics of sharing resources and responding in a multi-agency, coordinated and effective manner is further intensified by the geographical size of Canada and the remoteness of some areas.

Key Guidelines for PSS in Canada

The following discussion introduces the source of guidelines in the area of PSS. Examples are used to illustrate those relevant to emergency management.

1. Legislation:

Legislation surrounding emergency management is an important component to understand, as most emergency management organizations are mandated through legislation to operate within defined parameters. Some of the more pertinent legislation includes, but is not limited to:

- *Federal Emergency Preparedness Act and Emergencies Act*
- *National Defence Act*
- *The Anti-terrorism Act and Federal Bill C-36*
- *Security Offences Act*
- *Official Secrets Act*
- *Federal Bill C-45⁸²*
- *Provincial/Territorial Emergency Measures Acts*
- *Municipal Emergency Acts*

2. Emergency Response Plans (ERP):

New legislation, such as Federal Law C-45, has mandated every organization to have an emergency management program. The plans set out a structure for roles and responsibilities in emergency situations, and should be a useful tool for interagency collaboration. However, there are no standards for format, content or level of detail, thus, the presentation of the information, the type of information and the methods for gaining access to information is different for each organization and agency. This "Pandora's

⁸² An act which amends the criminal code to clearly define who is responsible for the safety of persons in the workplace and to allow for prosecution under charges of "criminal negligence" when those responsibilities are recklessly or willfully disregarded.

box” is very difficult to navigate through and does little to enhance the understanding between stakeholders.

3. Memorandums of understanding (MOUs) and Mutual Aid Agreements (MAAs):

MOUs and MAAs are becoming increasingly common as organizations come to grips with the challenges of emergencies that are beyond their ability to respond to as stand-alone entities. Canadian MOUs include:

- *The RCMP and Department of National Defense Joint NBC Defense Company (currently under review).*
- *A tri-city CBRN response team collaboration between Windsor, Toronto and Ottawa.*

4. Government Policy:

The following policy documents provide guidelines in the area of PSS to provide a national framework:

- *National Security Policy*
- *National Strategy for Critical Infrastructure Protection*

6. Military Doctrine:

Domestically, the Canadian Forces (CF) do not have an “emergency response plan” as do the other governmental departments. The document *CF Operations* (B-GG-005-004/AF-00) is the keystone manual within the CF doctrine publication system and it concentrates on the operational level of force employment, where emphasis is placed on the synergistic integration of CF commands and agencies so that their total effort can be concentrated decisively to achieve the commander’s mission. Much of the text is applicable to domestic response and civil-military cooperation that are an integral part of PSS. In domestic PSS situations, the CF may act in support of other federal agencies, and provincial or municipal agencies within the parameters of three main legal mechanisms: Provision of Service, Aid of the Civil Power and Assistance to Law Enforcement Agencies. Rarely would the CF act unilaterally as the lead agency. The CF is involved in routine operations such as counter-drug and maritime security with agencies such as the RCMP, Canadian Border Security Agency, Transport Canada and the Coast Guard. They can also be called upon for support to agencies such as the Fire Services in British Columbia for assistance with fighting forest fires.

7. Collaboration with the United States:

Due to the geographic positioning of Canada and the United States, the two countries collaborate in many areas of PSS to ensure the safety of citizens and critical infrastructures in both countries. The two countries are signatories to the Agreement Between the Government of the United States of America and the Government of Canada on Cooperation in Comprehensive Civil Emergency Planning and Management of April 28, 1986. Memorandums of Understanding (MOUs), such as the Canada-United States Joint Radiological Emergency Response Plan (JRERP), are intended to complement existing national, provincial, and state emergency plans. The joint response mechanisms between the two countries establish a framework for peacetime response assistance that is designed to alert federal authorities of potential or actual

threats, cooperatively reduce threats, and to facilitate support coordination of US and Canadian responders in the event of a PSS incident as required.

Critical Infrastructure Protection in Canada

In November 2004, PSEPC published a document titled: *Government of Canada Position Paper on a National Strategy for Critical Infrastructure Protection*. The position of this paper is “to create an integrated and forward-looking National Critical Infrastructure Protection Strategy that will include voluntary participation from industry stakeholders as well as from federal, provincial and territorial governments by the fall of 2005.” Due to the fact that 85% of all critical infrastructure is not government owned, but held by private interests, CIP in Canada involves a wide range of stakeholders and partners.

PSEPC has identified 10 infrastructures that are deemed “critical” to PSS: *energy and utilities; communications and information technology; finance; health care; food; water; transportation; safety; government; and manufacturing*.

A Note on the PSS landscape in the United States

On November 25, 2002 President George W. Bush created the Department of Homeland Security (DHS). The Department's mission is to prevent terrorist attacks within the United States, to reduce America's vulnerability to terrorism, and to minimize the damage and recovery required from attacks that do occur. In order to accomplish this mission, the Department places a high priority on inter- intra- and extra-governmental cooperation, coordination, and information sharing⁸³.

The DHS is the agency responsible for PSS in the United States. The DHS works with key organizations in the realm of PSS in the United States such as the Federal Emergency Management Agency (FEMA), the Information Analysis and Infrastructure Protection (IAIP) Directorate, and the private-public Partnership for Critical Infrastructure Security (PCIS). As in Canada, the Department of Defense (DoD) plays a role in defending and protecting America, and similarly, their activities are also most often conducted in support to first responders. In collaboration with numerous other federal and state agencies, the US organizations are designed to provide the framework necessary to protect their citizenry and critical infrastructure.

The U.S. Department of Homeland Security expects to play a significant role in such areas as IS and Sensor Networks. With a budget of nearly \$1 billion for the current fiscal year, ending in September, the emerging Science and Technology Directorate inside DHS is still relatively small by government standards, but observers say it is among the fastest-growing channels for federal R&D spending. The private-sector programs that will claim the bulk of that spending will be handled by the Homeland Security Advanced Research Projects Agency (HSARPA), roughly modeled on the Pentagon's successful Darpa program.

⁸³ http://it.ojp.gov/topic.jsp?topic_id=46, accessed 23 November 2004

References

- [10 Emerging 2004] 10 Emerging Technologies That Will Change Your World , Technology Review, February 2004
- [AAAI Law] Law Enforcement and Public Safety Topic Group Page in AAAI (<http://www.aaai.org/AITopics/html/lawenf.html>)
- [Adams 1998] James Adams, *The Next World War: Computers Are the Weapons and the Front Line Is Everywhere*. New York: Simon & Schuster, 1998, 368 pp.
- [Adams 2001] James Adams, *Virtual Defense*, Foreign Affairs, May/June 2001
- [Agence France 2005] Thousands Flee as Death Toll in Kenyan Water Clashes Rises. Agence France Presse , January 24, 2005
- [Albert Et. al 2000] R. Albert, H. Jeong, and A.-L. Barabási, Error and attack tolerance in complex networks, *Nature* 406 , 378 (2000).
- [Allsopp et al 2002] Allsopp, D.N., Beutement, P., Bradshaw, J.M., Durfee, E.H., Kirton, M., Knoblock, C.A., Suri, N., Tate, A. and Thompson, C.W. "Coalition Agents Experiment: Multi-Agent Co-operation in an International Coalition Setting", Special Issue on Knowledge Systems for Coalition Operations (KSCO), *IEEE Intelligent Systems*, Vol. 17 No. 3 pp. 26-35. May/June 2002.
- [Allsopp et al 2003] Allsopp, D., Beutement, P., Kirton, M., Tate, A., Bradshaw, J.M., Suri, N. and Burstein, M. (2003) *The Coalition Agents Experiment: Network-Enabled Coalition Operations*, Special Issue on Network-enabled Capabilities, *Journal of Defence Science*, Vol. 8, No. 3, pp. 130-141, September 2003.
- [Basalla 1990] George Basalla, *The Evolution of Technology*, Cambridge University Press, 1990
- [BBC News 2005] Developing world births 'falling', BBC News, Wednesday, 26 January, 2005
- [Beauchamp 2002] Jesse L. (Jack) Beauchamp, *Countering Terrorism: The Role of Science and Technology, A Personal Perspective*, *Engineering & Science*, 4, 2002, pp 26 –35.
- [Bennett 2003] Bennett, Bruce W. *Responding to Asymmetric Threats, New Challenges New Tools for Defense Decisionmaking*. Rand Corporation, Santa Monica, CA. 2003, pg 33-66. www.rand.org/publications/MR/MR1576, accessed February 2004.
- [BMO 2003] *Impact of 'Mad Cow' Disease on the Cattle-Beef Sector*, Report, BMO Financial Group, Bank of Montreal, November 29th, 2004. www.bmo.com/economic/
- [Bounagui et al 2004] Abderrazzaq Bounagui, Nouredine Bénichou and Ederne Victor, *Analysis of Fire Statistics in Canada 1986-2000*, the National Research Council of Canada, NRC-CNCR Research Report No. 172, October 26, 2004
- [Buchanan 2001] Buchanan, B. 2001, *Creativity at the meta-level*, *AI Magazine*.

- [Budzik and Hammond 2000] Budzik, J. and Hammond, K. 2000, User interactions with everyday applications as context for just-in-time information access. In Proceedings of the 2000 International Conference on Intelligent User Interfaces, pgs 44-51.
- [Carafano 2004] James Jay Carafano, Strategy and Security in the Information Age: Grading Progress in America's War on Terrorism, Heritage Lecture #824, March 17, 2004, <http://www.heritage.org/>
- [CDS 2000] Chief of Defence Staff. *Canadian Forces Operations*, B-GG-005-004/AF-000. OPI: J7 DLLS 2, Department of National Defence, Ottawa, Ontario, 2 October 2000.
- [CFR 2003] Council on Foreign Relations. *Emergency Responders: Drastically Underfunded, Dangerously Unprepared*. Report of an Independent Task Force sponsored by the Council on Foreign Relations, 2003.
- [Chandrasekaran et al.1999] Chandrasekaran, B.; Josephson, J.; and Benjamins, R. 1999., What are ontologies, and why do we need them? IEEE Intelligent Systems 14(1).
- [CMU listen 2004] Project Listen, <http://www.cs.cmu.edu/~listen/>.
- [Cohen1995] Cohen, H. 1995. The further exploits of AARON, painter. Stanford Humanities Review 4.
- [Comfort 2002] Comfort, Louise K. *Governance under Fire: Organizational Fragility in Complex Systems*, Symposium on Governance and Public Security, Campbell Public Affairs Institute, Maxwell School of Citizenship and Public Affairs, January 18, 2002, Syracuse University, NY.
http://www.maxwell.syr.edu/campbell/Governance_Symposium/comfort.pdf, accessed April 2004.
- [Conger 2004] Conger, John. *Unique CBRNE Training Issues Face Joint Task Force—Civil Support*, Journal of Homeland Security, ANSER, April 2004.
<http://www.homelandsecurity.org/journal/Articles/displayarticle.asp?article=111>, accessed April 2004.
- [Damian 2002] Lilly, Damian. *The Peacebuilding Dimension of Civil-Military Relations in Complex Emergencies*, International Alert, August 2002. www.international-alert.org/pdf/pubdev/briefing3.pdf, accessed March 2004.
- [Dean and Kambhampati 1997] Dean, T. and Kambhampati, S. 1997, Planning and scheduling, In The Computer Science and Engineering Handbook. CRC Press, Hillsdale, NJ, 614-636.
- [Economist 2003] The day the lights went out, the Economist, Aug 15th 2003.
- [Eilperin 2005] Juliet Eilperin. Fish Farming's Bounty Isn't Without Barbs, Washington Post, Monday, January 24, 2005; Page A01
- [Eurosurveillance]. George Gouvras , The European Centre for Diseases Prevention and Control, Eurosurveillance , Issue 3, Vol 9, 2004

- [Feigenbaum and Buchanan 1993] Feigenbaum, E. A. and Buchanan, B. G. 1993, Dendral and meta-dendral: Roots of knowledge systems and expert system applications. *Artificial Intelligence* 59:233-240.
- [Ford and Hayes 1998] Ford, K. and Hayes, P. 1998. On computational wings: Rethinking the goals of artificial intelligence. *Scientific American Presents* 9(4):78-83.
- [Frawley et al 1992] W. Frawley and G. Piatetsky-Shapiro and C. Matheus, Knowledge Discovery in Databases: An Overview. *AI Magazine*, Fall 1992, pgs 213-228.
- [FTC 2004] Federal Trade Commission, National and State Trends in Fraud and Identity Theft, January -December 2003, January 22, 2004.
<http://www.consumer.gov/idtheft/index.html>.
- [GAO-04-259T 2003] Bioterrorism, A Threat to Agriculture and the Food Supply Statement for the Record by Lawrence J. Dyckman, Director Natural Resources and Environment, Testimony Before the Committee on Governmental Affairs, U.S. Senate, United States General Accounting Office, November 19, 2003, GAO-04-259T
- [Gonsalves 2004] Cynthia E. Gonsalves, Dod Annual Report to Congress on Technology Transfer Programs, Presented at the FLC Mind-Atlantic Regional meeting, Cumberland, MD, September 16 2004.
- [Harrison] Harrison, Doug. *Ontario Provincial Emergency Response Plan*, Emergency Measures Ontario (EMO) presentation.
http://www.cpha.ca/ctph/prespdf/Doug_harrison.pdf, accessed March 2004.
- [Hearst and Hirsh 2000] Hearst, M. and Hirsh, H. 2000. AI's greatest trends and controversies, *IEEE Intelligent Systems* 15(1):8-17.
- [Hendler 1999] Hendler, J. 1999. Is there an intelligent agent in your future? *Nature Webmatters*.
- [Hoffman 2003] Hoffman, Bruce. *Al Qaeda, Trends in Terrorism and Future Potentialities: An Assessment*, RAND Corporation, Santa Monica, CA, 2003.
<http://www.rand.org/publications/P/P8078/P8078.pdf>, accessed March 2004.
- [Hofstadter 1985] Hofstadter, D. 1985. On the seeming paradox of mechanizing creativity. In *Metamagical Themas*. Basic Books, New York. 525-546.
- [InVS 2004] Abstract of the progress report on the heatwave 2003 in France, Institut de Veille Sanitaire (InVS) (the National Institute of Public Health Surveillance), Saint Maurice, France, www.invs.sante.fr
- [Jackson et al 2003] Brian Jackson, D.J. Peterson, James Bartis, Tom LaTourrette, Irene Brahmakulam, Ari Houser, Jerry Sollinger, *Protecting Emergency Responders: Lessons Learned from Terrorist Attacks*, CF-176-OSTP, 2002, ISBN: 0-8330-3149-X
- [Jackson et al 2004] Brian Jackson, John Baker, Susan Ridgely, James Bartis and Herbert I. Linn, *Protecting Emergency Responders Volume 3: Safety Management in Disaster and Terrorism Response*, Rand MG-170-NIOSH, 2004, ISBN: 0-8330-3556-8

- [James 2004] Geoffrey James , The Leadership Game, Business 2.0, May 18, 2004.
- [Jarvis et Al 2004] P. A. Jarvis, Teresa G. Lunt, K. L. Myers, Identifying Terrorist Activity with AI Plan Recognition Technology, AAAI 2004.
- [Kane 2003] Kane, John (Lt.). The Incident Command System and the Concept of Unified Command at a Terrorist Incident, Community Response to the Threat of Terrorism Symposium, Public Entity Risk Institute, Fairfax VA. January 2003. http://www.pep.bc.ca/hazard_preparedness/Symposium_Paper-Unified_Command.pdf, accessed July 2004
- [LaTourrette et Al 2002] Tom LaTourrette, D. J. Peterson, James T. Bartis, Brian A. Jackson, and Ari Houser, Protecting Emergency Responders, Volume 2: Community Views of Safety and Health Risks and Personal Protection Needs, MR-1646-NIOSH, 2003, ISBN: 0-8330-3295-X
- [Leake 1996] Leake, D. 1996. CBR in context: The present and future. In Leake, D., editor 1996, Case-Based Reasoning: Experiences, Lessons, and Future Directions. AAAI Press, Menlo Park, CA. 3-30.
- [Leake 1998] Leake, D. 1998. Cognition as case-based reasoning. In Bechtel, W. and Graham, G., editors 1998, A Companion to Cognitive Science. Blackwell, Oxford. 465-476.
- [Leake and Kolodner 2001] Leake, D. and Kolodner, J. 2001. Learning through case analysis. In Encyclopedia of Cognitive Science. Macmillan, London.
- [Leggiere 2004] Leggiere, Philip. "More Data, Less Noise", HS Today, 1(7): 23-27, November 2004. KMD Media: McLean, VA.
- [Leggiere 2004] Leggiere, Philip. "More Data, Less Noise", HS Today, Vol 1, No 7, November 2004. KMD Media: McLean, VA. Pg 23-27.
- [Lenat 1979] Lenat, D. 1979. On automated scientific theory formation: A case study using the AM program. In Hayes, J.; Mitchie, D.; and Milulich, L., editors 1979, Machine Intelligence, volume 9. Halsted Press.
- [Lenat 1995] Lenat, D. 1995. A large-scale investment in knowledge infrastructure. Communications of the ACM 38(11):33-38.
- [McCarter 2004] McCarter, Mikey. "Training Against Trouble", HS Today, 1(7): 12-18, November 2004. KMD Media: MaLean VA.
- [Mena 2004] Jesus Mena, Homeland Security as Catalyst: New Technology for Intelligent Analysis, Intelligent Enterprise, July 2004 (<http://www.intelligententerprise.com/showArticle.jhtml?articleID=22102265>)
- [Merritt 2003] Rick Merritt, "Sensor Nets Top R&D List for Homeland Security Agency," EE Times, December 31, 2003, at <http://www.eetimes.com/story/OEG20031231S0006>.
- [Muehlencamp 2005] www.muhenkamp.com/methods/html/ssrevisited.html, Muehlencamp & Company, Inc. www.muhenkamp.com

- [Munchener] Munchener Ruck / Munic Re Group, www.munichre.com/
- [NCAR] National Center for Atmospheric Research (NCAR)
- [Newell and Simon 1976] Newell, A. and Simon, H. 1976. Computer science as empirical inquiry: Symbols and search. Communications of the ACM 19:113-126. Reprinted in Haugeland, J., ed, Mind Design II, MIT Press, 1997.
- [NIA 2050] National Institute on aging, www.nia.nih.gov.
- [NRC-USDE 2004] Blackout One Year Later: Actions Taken in the United States and Canada To Reduce Blackout Risk Report to the U.S.-Canada Power System Outage Task Force Natural Resources Canada U.S. Department of Energy, August 13, 2004
- [NS EMO] Nova Scotia Emergency Measures Organization (NS EMO). *Emergency Management Manual*, Nova Scotia Emergency Measures Organization. <http://www.gov.ns.ca/emo/tools/download/manual.pdf>, accessed March 2004.
- [PCO 2004] Privy Council Office. *Securing an Open Society: Canada's National Security Policy*. Privy Council Office, Ottawa, Ontario. April 2004. http://www.pco-bcp.gc.ca/docs/Publications/NatSecurnat/natsecurnat_e.pdf, accessed August 2004
- [Pomerleau and Jochem 1996] Pomerleau, D. and Jochem, T. 1996. A rapidly adapting machine vision system for automated vehicle steering. IEEE Expert 11(2):19-27.
- [Portsmouth 2002] Ian Portsmouth, 20 bold predictions for the next 20 years, Profit Magazine, May 2002
- [PSEPC 2004] Public Safety and Emergency Preparedness Canada. Government of Canada Position Paper on a National Strategy for Critical Infrastructure Protection, November 2004. http://www.ocipep.gc.ca/critical/nciap/positionpap_e.asp, accessed November 2004.
- [Russell and Norvig 1995] Russell, S. and Norvig, P. 1995. Artificial Intelligence: A Modern Approach. Prentice Hall, Englewood Cliffs, NJ.
- [Samuel 1963] Samuel, A.L. 1963. Some studies in machine learning using the game of checkers. In Feigenbaum, E.A. and Feldman, J., editors 1963, Computers and thought. McGraw-Hill. Also in IBM Journal of Research and Development (1959).
- [Schank and Leake 1989] Schank, R.C. and Leake, D. 1989. Creativity and learning in a case-based explainer. Artificial Intelligence 40(1-3):353-385. Also in Carbonell, J., editor, Machine Learning: Paradigms and Methods, MIT Press, Cambridge, MA, 1990. Project information is on-line at <http://www.cs.indiana.edu/~leake/projects/swale>
- [Serious Games 2004] <http://www.seriousgames.org/>.
- [Steele 2001] Steele, Klara. *Terrorism Response Generating Unprecedented Levels of Co-operation*, Gazette, Royal Canadian Mounted Police: Vol 63, No6, 2001. http://www.rcmp.ca/gazette/gazette_vol63no6_e.pdf, accessed March 2004.

- [Turing 1950] Turing, A. 1950. Computing machinery and intelligence. Mind 59. Reprinted in J. Haugeland, Ed., Mind Design II, MIT Press, 1997.
- [Tuzzolo 1997] Tuzzolo, John J., The Challenge of Civil-Military Operations, Joint Force Quarterly, Institute for National Strategic Studies, National Defense University no. 16 (Summer 97), pp. 54-58 http://www.dtic.mil/doctrine/jel/jfq_pubs/balkan4.pdf, accessed July 2004.
- [US DoJ 2004} US Department of Justice. "Information Technology Initiatives" http://it.ojp.gov/topic.jsp?topic_id=46, accessed 23 November 2004
- [Wagner et Al] T. Wagner, J. Phelps, V. Guralnik, R. VanRiper, An Application View of COORDINATORS: Coordination Managers for First Responders, AAAI 2004.
- [Walkerton-2005] Walkerton E. Coli Tragedy, Canoe C-Health, 2005, <http://www.canoe.ca/EcoliTragedy/home.html>.
- [Wiederhold 1986] G. Wiederhold, "Knowledge versus Data,
- [WWI 1999] World Watch Institute State of the World 1999 Jan 1999.
- [McCarter 2004] McCarter, Mikey. "Training Against Trouble", HS Today, Vol 1, No 7, November 2004. KMD Media: MaLean VA, pg 12-18.