



# Public Safety Major Project

2008 – 2010 SMP Briefing Document.

## i. Introduction

---

During 2007, four new Major Projects were defined by groups of academic and industry volunteers following consultations of companies with respect to their interests in terms of research partnerships with academia. These briefing documents circumscribe, albeit with a relatively broad scope, the themes of interest for the 2008-2010 Major Projects. The purpose of this document is to propose scientific research themes related to the **Public Safety Major Project**.

Prompt thanks all academic and industry volunteers who participated in this process, and particularly those individuals who were tasked with drafting the briefing documents for their efforts on behalf of our ICT community.

## ii. Table of Content

---

<b>I. INTRODUCTION</b>	<b>1</b>
<b>II. TABLE OF CONTENT</b>	<b>1</b>
<b>1. THE CONCEPT OF "MAJOR PROJECT"</b>	<b>2</b>
<b>1.1 AD-HOC COMMITTEE</b>	<b>2</b>
<b>2. DEFINING "SECURITY"</b>	<b>3</b>
<b>3. KEY RESEARCH AREAS</b>	<b>4</b>
<b>3.1 PREVENTION</b>	<b>4</b>
<b>3.2 INTERVENTION</b>	<b>5</b>
<b>3.3 THE HUMAN FACTOR</b>	<b>5</b>
<b>3.4 INFORMATION FUSION</b>	<b>6</b>
<b>4. SPECIFIC RESEARCH INTERESTS</b>	<b>6</b>
<b>4.1 TECHNOLOGICAL FIELDS</b>	<b>6</b>
<b>4.2 CONTEXTUAL FIELDS</b>	<b>7</b>
<b>5. GRANT COMPETITION DEADLINES</b>	<b>8</b>

## 1. The Concept of “Major Project”

The broad perspective of the here below described research challenges can be summed up in three primary orientations creating a “research perimeter” covering a multitude of more specific themes. The **Public Safety Major Project** thus targets a strategic grouping of focused specific research projects that derive their coherence from within the perimeter. Its topography highlights the fields; main areas for research identified through extensive committee discussions. In addition, a regulatory and commercial perspective acting as a socioeconomic beacon further circumscribes the relevance of specific research projects to be proposed. As such, a non-exhaustive list of emerging technologies and challenging fields from within the research perimeter is presented at the end of this document. Specific project proposals are sought to explore not only one of the major fields of the perimeter but also the overlaps across these fields.

Research proposals will be required to emphasize delivery of results (outcome-based research); technologies, applications, systems, etc... mature enough to meet the interests and requirements of industry partners. It is also understood that the integration and demonstration objective of this overall major project may also lead to modifications of the proposal’s specific deliverables.

### 1.1 Ad-Hoc Committee

The definition of the research perimeter results from a dialogue between the industry and academic partners. The following representative of both domains have been directly involved in the discussions, as well as into the reviewing process, which led to the creation of the present document.

<b>François Gagnon</b> (committee co-chair)	École de technologie supérieure
<b>Richard Cayouette</b> (committee co-chair)	Ultra Electronics TCS
<b>Iwan Jemczyk</b> (committee co-chair)	Ultra Electronics TCS
<b>Denis Akzam</b>	Parallel Geometry Inc.
<b>Nicolae Alecu</b>	Parallel Geometry Inc.
<b>Louis Fortier</b>	CRIM
<b>Claude Lévesque</b>	Technopôle Défense & Sécurité
<b>Emerson Nerat</b>	Purelink Technology
<b>Alex Stephenne</b>	Ericsson Canada
<b>Charles Despins</b>	Prompt

<b>Soroush Amidi</b>	Honeywell
<b>Naïm Batani</b>	ISR Technologies
<b>Jules Bélair</b>	IBM Bromont
<b>Alan Bernadi</b>	Bell University Labs
<b>Dave Dietz</b>	Research In Motion
<b>Charles Goyette</b>	MDEIE
<b>Olivier Munger</b>	École de technologie supérieure
<b>André Parent</b>	Institut National d'Optique
<b>Djemel Ziou</b>	Université de Sherbrooke

## 2. Defining “Public Safety”

[Global Theme]

Since September 2001, “Homeland Security” is commonly referring to a country’s national and synchronized effort involving all the relevant governmental agencies in order to protect its territory and its inhabitants against hazards, whether internal or external, from both natural and man-made sources. Therefore, the definition has been compressed and extended many times; following the fluctuations of the homeland security emerging market. On one side, as define by the United States’ *National Strategy for Homeland Security*<sup>1</sup>, it focuses quasi exclusively on terrorism deterrence and fighting. While, from another side it is made more inclusive and refers to the protection of nations (people, resources, infrastructures and territory) against “all” possible threats. The Government of Canada and the Government of Quebec use the terms “public security”, “public safety”, and “civil protection” to mean “Homeland Security”.

From Prompt’s perspective, in order not to set restrictive boundaries and prevent the channelling of scientific creativity, we refer to a wider and more inclusive definition of global security. Therefore, the scope of the Public Safety Major Project includes the following aspects:

- **Emergency preparedness, responses, and lessons learned whether confronting manmade or natural disasters.**
- **Domestic intelligence.**
- **Critical infrastructure protection.**
- **Border security.**
- **Transportation security.**

<sup>1</sup> Office of Homeland Security, « The National Strategy for Homeland Security », July 2002.

- **Detection and defence against biological, chemical, nuclear materials and weapons.**
- **Interoperability for first responders, and in between agencies**

Sub-sections 4.1 and 4.2, located at the end of the present document, propose a list of concrete and specific themes for which the “application potential” has been confirmed by the Ad-hoc Committee.

## 3. Key Research Areas

---

### 3.1 Prevention

---

While most people will agree on the fact that 100% efficiency remains a driving goal, crisis avoidance is nonetheless a key element within the global homeland security strategy. What can be prevented should be evaded. This leads to two strategic questions: identifying the “what”, and finding “how” to prevent it. Effort should be put forward in order to identify infrastructure dependencies in its very wide sense. There are weaknesses lying within the dependencies between information technologies and data storage, power generation and distribution grids as well as urban infrastructures, highways, railroads and airports. The “domino effect” must be containable to the highest possible extent in order to maximize the response time and the overall in-crisis intervention efficiency. Strategies oriented on simulation-based planning are already foreseen as an effective tool for minimizing the dependency weakness.

Another axis for prevention resides in the localization and management of identities: humans and assets. Not without raising many questions when it comes to personal privacy, the “omniscience” ultimately provided by technologies for identification, localization and tracking is yet a doubly useful tool. Of course, knowing “where is who” is a potential threat locator as much as a lifeline for people lost or in need when facing adversity. The material part of such axis also brings the traceability notion. With the increasing amount of Asia based outsourcing of strategic components such as the microprocessors populating the zillions of computers distributed across the planet, combining traceability and data integrity must be part of the security strategy. For example, the possibility that a silicon foundry, from one country, produces FPGAs<sup>2</sup> and DSPs<sup>3</sup>, to be used in the military modules of another country, which integrates back door circuitry and/or Trojan horse type software, implies very critical issues. Thus, the capability to join traceability information with data integrity status would enable the end user country to verify that the production pipeline has not been hacked or modified.

---

<sup>2</sup>Field Programmable Gate Arrays.

<sup>3</sup>Digital Signal Processors.

### 3.2 Intervention

---

Unfortunately, until prevention mechanisms yield an efficiency ratio of more than the proverbial “five nines”, humanity must be ready and equipped to confront threats. As for a paramedic intervention in a heart failure situation, the effectiveness of the response to a disaster is critical for minimizing the impact of such event. Reconstructing or deploying a makeshift communication system may represent an exceedingly complex mission. Indeed, connecting many different services which are independently equipped with different communication technologies rapidly becomes a nightmare. The level of adaptability required to assume a high level of interoperability is very high. The military forces have been dealing with fast deployment for a very long time and, throughout the last decade or so, they invested a lot of money and effort in orienting their equipment roadmap toward cognitive radio. Seen as the next step of evolution from the software defined radio (SDR), cognitive radios will integrate the capacity of being aware of their operational environment and then accordingly optimize their configuration. Such a communication device could for instance “understand” the difference between time of peace and time of crisis in order to modify its adaptation criterions. Such basis for adaptation represent itself a challenge because of the difference degree between the operational rules when recovering from disasters. For example, radio spectrum should be allocated according to a completely different quality of service table as well as to maximize the survivability of the connections.

Notwithstanding the ICT orientation of the HS Major Project, there are no communication networks that will stand alone without having the proper level of energy supply. Not exactly an issue for the communication backhaul context, energy rapidly becomes one when it comes down to the survival of small wireless devices. Wireless sensors, and wireless sensor networks are good examples of where low power consumption meets with energy harvesting and wireless distribution. Whether for a large piece of equipment or for a cloud of smart dust sensors, efficient energy usage will always remain a strategic element during times where rationalized resource consumption is of the essence.

### 3.3 The Human Factor

---

When fighting disasters, the human factor is usually associated to chaotic response or at least with non-deterministic behaviours. Even highly trained people like army troopers, law enforcement officers or fire fighters face great difficulties when the call relates to the emotional duty of protecting their homeland and families. The stress factor should not only be a matter of efficient management during crisis but also be considered when simulating and planning responses.

Of course, all the man made types of disasters have something in common: their human origin. As the meteorologists monitors the behaviours of atmospheric fluids to extrapolate weather forecasts, analysis of the human factor is a way of scrying into malicious intentions. By using enhanced behaviour identification algorithms with tridimensional facial recognition softwares, both capable of working under dense crowded condition, we can expect to pinpoint terrorists in action.

### 3.4 Information Fusion

---

Nowadays, sensing technologies enable the acquisition of a very wide spectrum of stimuli. The collateral effect of deploying so many ears and eyes is the tremendous quantity of data generated and waiting to be analysed. Getting the information is not the problem, but processing it, is. In addition, the different formats or type of data makes the gathered information very heterogeneous and even harder to process. Data fusion technologies emerged from this increasingly difficult problem and propose ways of solution. However, much work is required until such new data management and processing schemes can be integrated in security applications.

The advent of digital technologies and wireless communication literally consecrated the electronic warfare as a new vector of attack/defence. Although peoples agree on the fact that electronic aggression are less damageable in terms of human losses than the other vectors (air, water and land), it doesn't reduce its threat potential. Very malicious, stealthy, concealable and relatively inexpensive, a breach in the information exchange security could lead to critical hits. Therefore, information protection is one of the top priorities. For example, strategies for data anonymization are one of the promising ways for making the in-transit data unappealing for hackers. Combined with improved encryption algorithms and with reliable integrity sentinels, the transaction of sensitive data becomes more and more impervious to digital pirate crimes.

On the other side, law and order agencies will concurrently seek a second and diametrically opposed objective: in-packet investigation. By monitoring the content or clear data, of the information exchange on communication platforms such as the Internet or cellular networks, prevention of manmade disastrous acts is much easier. Assuming that the agencies have means for processing such a payload of information. However, unless governmental agencies are holding all the keys, both quests are facing complete contention. And giving all the keys to these agencies brings, yet again, the personal privacy problem on the table. The handling of information brings great challenges which are far from being circumscribed to the technology domain. A good understanding of the socio-cultural factors while developing innovative data security mechanism is probably a good starting point for increasing the level of security of the electronic vector.

## 4. Specific Research Interests

---

[Expressed by the industrial community]

### 4.1 Technological fields

---

- Tri dimensional facial reconnaissance in crowded situation.
- Robotic intervention.
- Identity management within unregulated (twilight) zones.
- Sensors improvement and new data acquisition devices and strategies.
- Energy harvesting.

- Sensitive data hiding, anonymity, transportation and manipulation.
- Cognitive radio technology to include network extension for coverage, dynamic access to spectrum, dynamic prioritization, dynamic network configuration to include non-first responders.
- Reliable, in situ chemicals and gases teledetection methods and apparatus.
- Retinal scanning and high efficiency biometric identifiers.
- Tri dimensional geo location of non-tagged personnel and assets.
- Location based services.
- Emergency response: deployment, intervention, and post deployment and lessons learned (knowledge management).
- Emergency Alert systems for affected populations.
- SDR and cognitive radios: the building blocks for crisis response deployment.
- Crisis network deployment: omnipresence of interoperability. Not only the technology, but the five (5) elements or dimensions of the interoperability continuum (governance, standards operating procedures, technology, training & exercises/simulations, and usage).
- Infrastructure survivability.
- Geospatial representations of floods, fires, storm ... but also the 3D representations of underground city tunnels for first responders in urban areas.
- In-crisis metrics and schemes for quality of service adaptation.
- Data fusion and processing.
- Artificial intelligence softwares for data analysis and exploration.
- Deep data investigation.
- Incident management systems and applications.
- Behavioural observation and pre-emptive intervention.
- "Human factor" based information management and dissemination.

## 4.2 Contextual Fields

---

- The Airport scenario.
- The first responders on a crisis or emergency scenario.
- Wide and low-population border surveillance.
- The rising migration of microelectronic key players toward developing countries while most of the security concerns remain an occidental affair.
- Vulnerability assessment and business case evaluation.



- Positioning the small players in a market driven by large corporations.
- Consideration of Canada – Quebec specific threat and prevention issues.

## 5. Grant competition deadlines

---

1. **June 11th 2008:** information and networking workshop.
2. **September 19th 2008:** deadline to submit letters of intent to Prompt.
3. **November 14th 2008:** deadline to submit detailed proposals to Prompt.