GENERAL DYNAMICS
Canada

Enabling Interoperable Public Safety Communications

A Primer for Development of a National, Secure Mission-Critical Network

Abstract

To be effective in the future, Canadian public safety and security personnel need completely interoperable communications networks, which leverage current and emerging hardware, software, analytical tools and end user applications to enable continuous, real-time, in-field access to critical information. A truly Canadian interoperable public safety network can be created by leveraging current governance frameworks, technology interoperability and analytical tools, and the best practices of all agencies. Implementation should complement existing governance, processes and technologies and capitalize on new technologies as they emerge. This will enable individual agencies to deploy and use more advanced tools for their geography and establish the processes that will enable interoperability as needed with other agencies including those in the United States.

Table of Contents

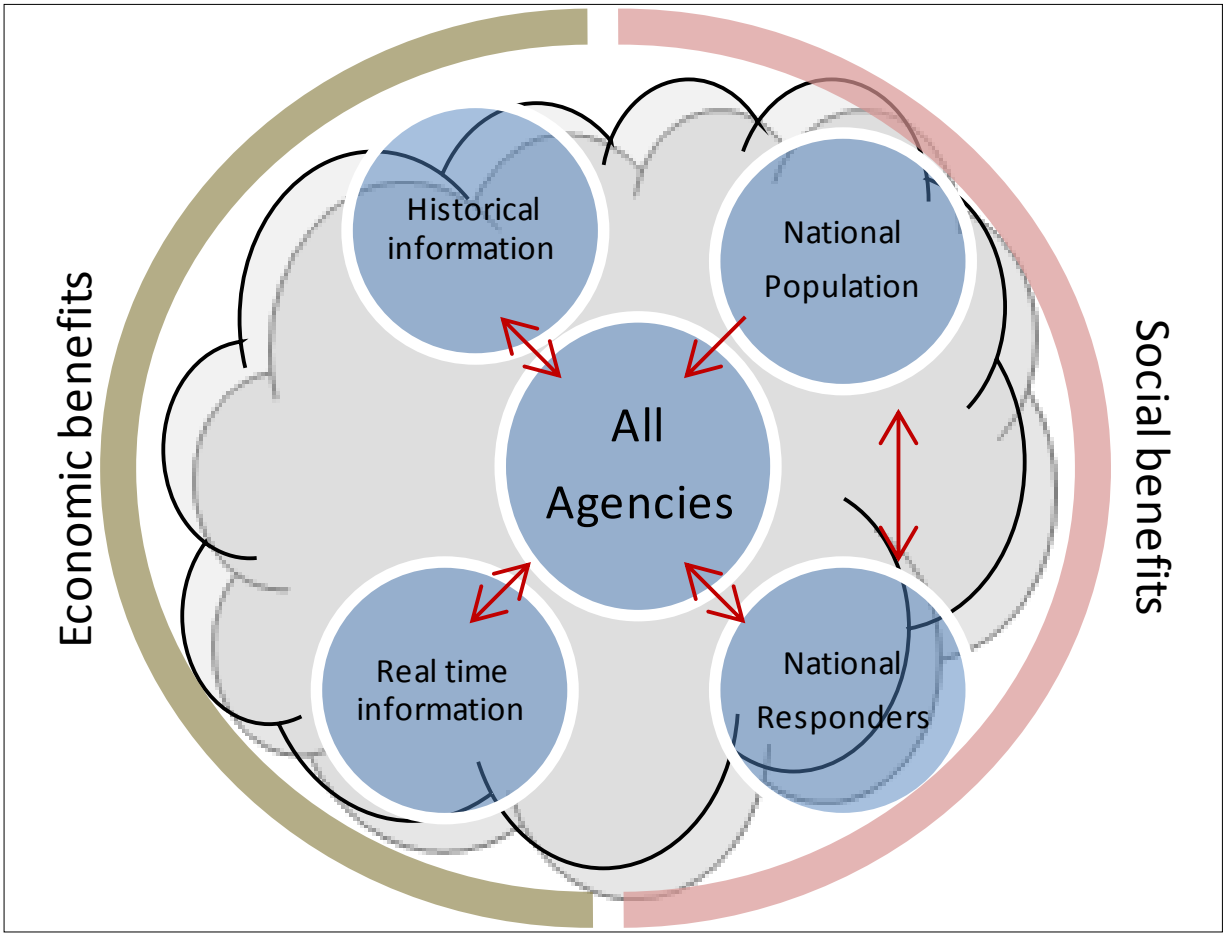
List of Illustrations

An Opportunity to Shape the Future

The effectiveness of public safety systems has been measured and tested in many different ways over the years. During that time, evolutionary trends have continued to move public safety processes from a reactive response state to a predictive, fully aware state. With full awareness, first responders can operate in safety and with confidence, and draw upon a greater number of resources on the front line.

Lifting a little of the fog from the national public safety cloud shows basic building blocks geared to increase Return on Investment (ROI) and social benefits while moving public safety processes to a fully aware state (Figure 1). Historical data gathered over many years about previous responses can be used to establish contextual information about any situation. Video cameras and other real time feeds can provide immediate intelligence about a situation, which can then be used by responding agencies to better inform first responders and provide them with everything they need to better protect themselves and do their job as they approach any situation.

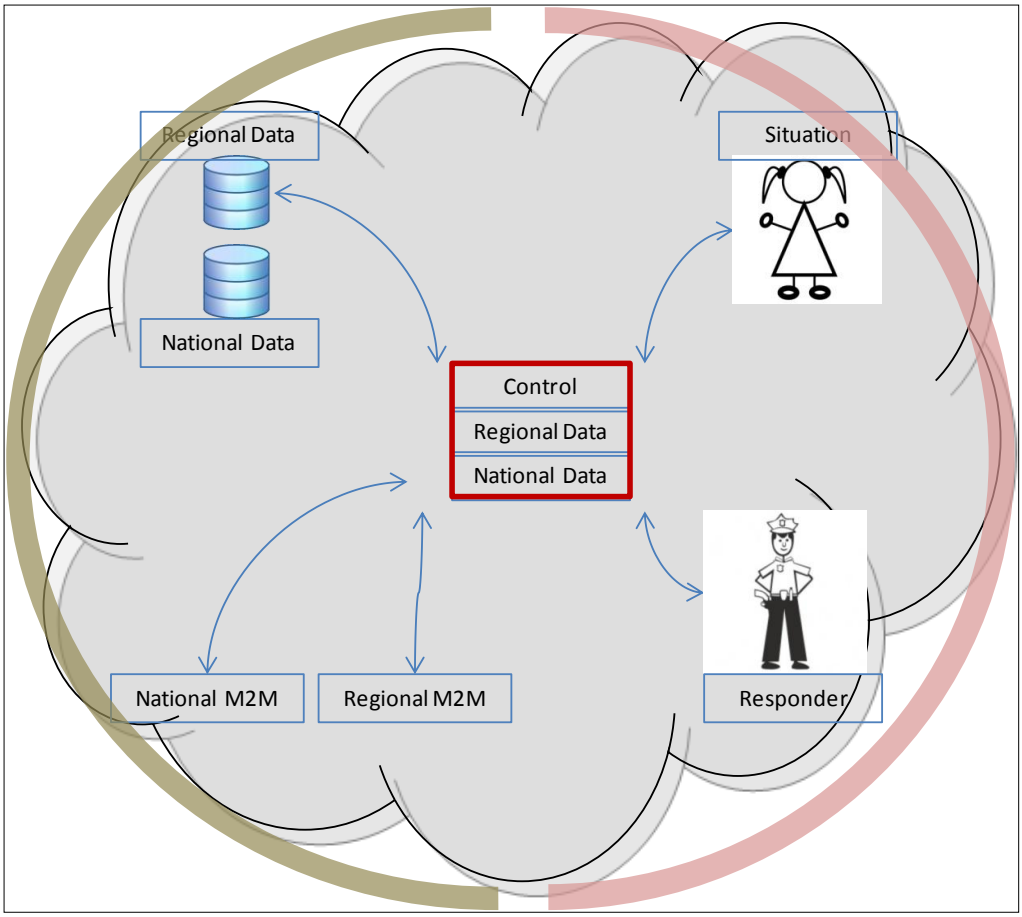
Figure 1: The basic building blocks of effective public safety.



First responders can never be 100 percent fully prepared for all situations at all times. But by leveraging the tools and intelligence available they can operate proactively rather than reactively.

For example, in most situations a dispatcher answering a 911 call records relevant details and then sends the appropriate emergency service unit to the location of the call. It's a simple process based on the dispatcher's ability to collect and relay as much information as possible to first responders by querying regional and national databases. If the caller does not describe the situation correctly, first responders could find themselves in a situation they are not prepared for. Today, dispatchers mix regional data and national data with 'in-location' data, such as surveillance camera feeds, to piece together relevant details of a situation in real and near real time (Figure 2). To improve this process and move towards a more proactive model, the system can be configured to use the 911 call to query a number of regional and national databases, pinpoint the caller's location and trigger any and all cameras available in the area. In this way, the dispatcher could relay historical and real time situational intelligence to first responders while they are en-route, thereby making them fully aware of the situation they are about to face. This proactive state also enables other responders to be better prepared should the situation escalate.

Figure 2: Dispatchers piece together information from various sources to establish accurate situational awareness.



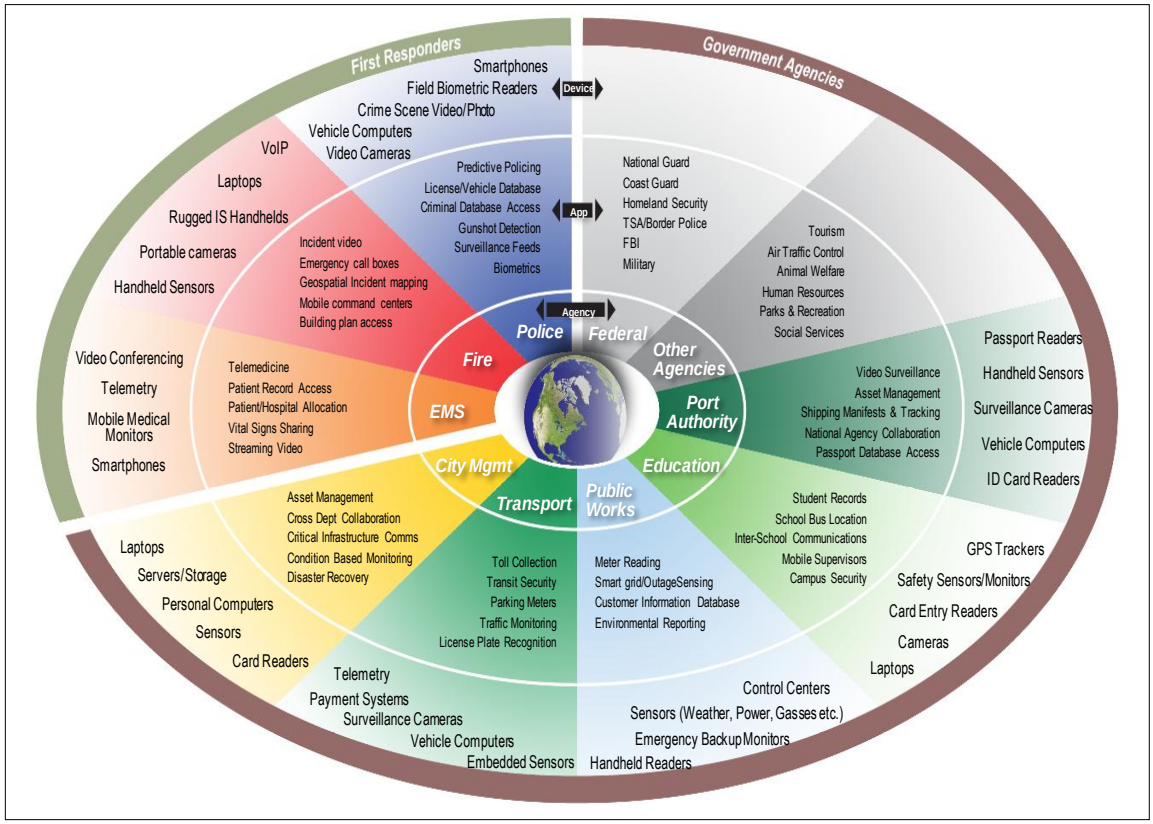
Evolution is not new to public safety agencies and Canada's public safety agencies stand on the threshold of a new era. Advances in technology have provided an opportunity to upgrade communications networks with new capabilities geared and designed to enhance the safety and effectiveness of first responders in any situation. At the same time, portions of the 700 MHz radio spectrum have been freed up for use by public safety and security organizations. Used effectively, this spectrum can be leveraged to create an interoperable wireless network that supports advanced machine-to-machine (M2M), multimedia devices and applications to enable more inter-agency collaboration and improve the efficiency of all public safety operations.

The type of communications systems required to cover the country nationally with common tools and regionally with specific tools that reflect the demographic and geographic needs of public safety agencies can be split into four distinct categories. Each category requires very different communications networks to support the complete array of first responder use cases:

- **Human-to-Human (H2H)** voice-based communications between people. This includes any communications between two people with information communicated for help or assistance. This could be between a person needing aid or help and a dispatcher, or between a first responder and dispatcher. For example, a dispatcher sending real time voice and video from a situation to another dispatcher or a group of responders irrespective of location.
- **Human-to-Machine (H2M)** communications between a dispatcher or responder querying databases. This includes basic processes, such as a driver license swipe against one or multiple databases for current information pertinent to a situation.
- **Machine-to-Human (M2H)** communications that involves a database sending feedback to a first responder based on a predefined or real time query. This may include a video surveillance camera sending live images to a first responder, or a real-time map of all responders from dispatch.
- **M2M** communications, such as that between video cameras, shot detectors, movement detectors, or a slew of sensors that form the additional eyes and ears of first responders in areas that they cannot be. This may include sensors from industry, manufacturers, shops, and Automated Teller Machines (ATMs), to build a grid of eyes and ears.

From the first responder M2M diagram (Figure 3) it is apparent that there is a large volume of real-time information available from agencies, applications, and devices that can be used to add situational intelligence to historical contextual database information. All this can be managed by a dispatcher and controlled to ensure that a situation is addressed to the best abilities of all resources, and that first responders are fully aware and safe in all situations.

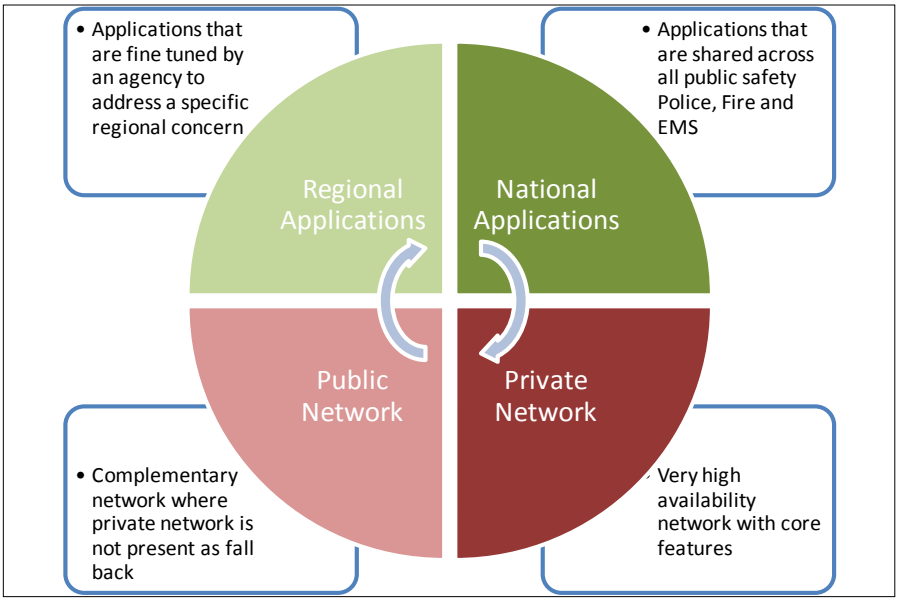
Figure 3: There is a large volume of real-time information available from agencies, applications, and devices.



The impact on the effectiveness of first responders is considerable. To capitalize on this, many countries have set aside a portion of the available radio spectrum to support more advanced information sharing by public safety agencies. The allocation of the 700 MHz spectrum in the United States has accelerated efforts focused on developing and deploying a nationwide interoperable network with a substantial commitment by government. Using a 99 percent population coverage model, deployment of this network will require approximately $6.5 billion in capital expenditure in 2010 dollars over ten years. Ongoing costs are expected to peak at as much as $1.3 billion per year. And the total cost over the next 10 years is estimated at approximately $12-16 billion, weighed against operational advancements and financial savings in the order of billions per year capped with scalable and evolvable networks.

It is unlikely that federal funding at this level will be set aside to create a similar network in Canada. But a uniquely Canadian, nationwide, interoperable wireless network is extremely important. Efficient information sharing through interoperable communications networks is the key to public safety and security in Canada. To be effective in the future, public safety and security personnel need completely interoperable communications networks, which leverage current and emerging hardware, software and end user applications from the military and consumer sectors to enable continuous, real-time, in-field access to critical information in crisis situations as well as when the network gracefully degrades (Figure 4).

Figure 4: Public safety and security personnel need completely interoperable communications networks, which leverage current and emerging hardware, software and end user applications.



However, building the networks and providing the applications are not the biggest challenges. Every element of public safety will be on an independent evolutionary path where networks, devices, applications, use cases, acceptability, and usability must all evolve regionally and nationally and at different stages.

The most difficult challenge is to establish governance that is loose enough to evolve and not too tight to stop innovation. Governance and policy frameworks that enable accountability and interoperability regionally and nationally are the key.

But the current and past policies of municipal, provincial, and federal governments, combined with the independent practices and procurement processes of public safety and security organizations have created a collection of siloed communications networks incapable of efficient interoperability. At the same time, limited technology and no common national spectrum have created capability gaps and a major stumbling block on the road to completely interoperable public safety communications networks.

Public safety organizations across the country agree that a Canadian effort can only succeed if it involves multiple stakeholders from government, academia, and industry. Organizations such as the Canadian Advanced Technology Alliance (CATA), the Canadian Interoperability Technology Interest Group (CITIG) and others have created a collaboration between public safety agencies and private enterprises, including telecommunications companies, focused on making effective use of the available wireless spectrum in a time of crisis and peace when the spectrum is not heavily utilized. Through collaboration, all stakeholders can explore how best to leverage available and emerging technologies and advanced capabilities.

Understanding the Interoperability Challenge

As noted by SAFECOM, a communications program of the United States Department of Homeland Security's Office for Interoperability and Compatibility, communications interoperability for public safety refers to "the ability of public safety agencies to share information across disciplines and jurisdictions exchanging voice and/or data with one another on demand, in real time, when needed, and as authorized".[1] This means that all groups — police, fire, paramedics — should be able to communicate with each other using the same technology and interoperable network in any emergency situation.

Unfortunately, this level of interoperability does not exist in Canada. In some Canadian cities the Land Mobile Radio (LMR) systems used by public safety groups are the primary communications tool and do not support interoperable communications. The systems in use are different from one agency to another. Likewise, data systems are proprietary. Typically, both these systems are incompatible, and, in some cases, aging. But with the right technology framework, multimedia systems that can take advantage of the latest applications for finance and social benefits and evolve to best address response situations can be deployed.

In addition, there are a variety of networks in use. Most are primarily point-to-point (LMR), broadcast (P25), or ad hoc (Wi-Fi®). These networks are still needed and are the best for their application, but they are not designed to easily support interoperability. As a result, to enable interoperability between agencies on the frontline today, in-field public safety personnel most often resort to exchanging communications equipment: a fireman will exchange a radio with a policeman, or a policeman will exchange a radio with paramedic.

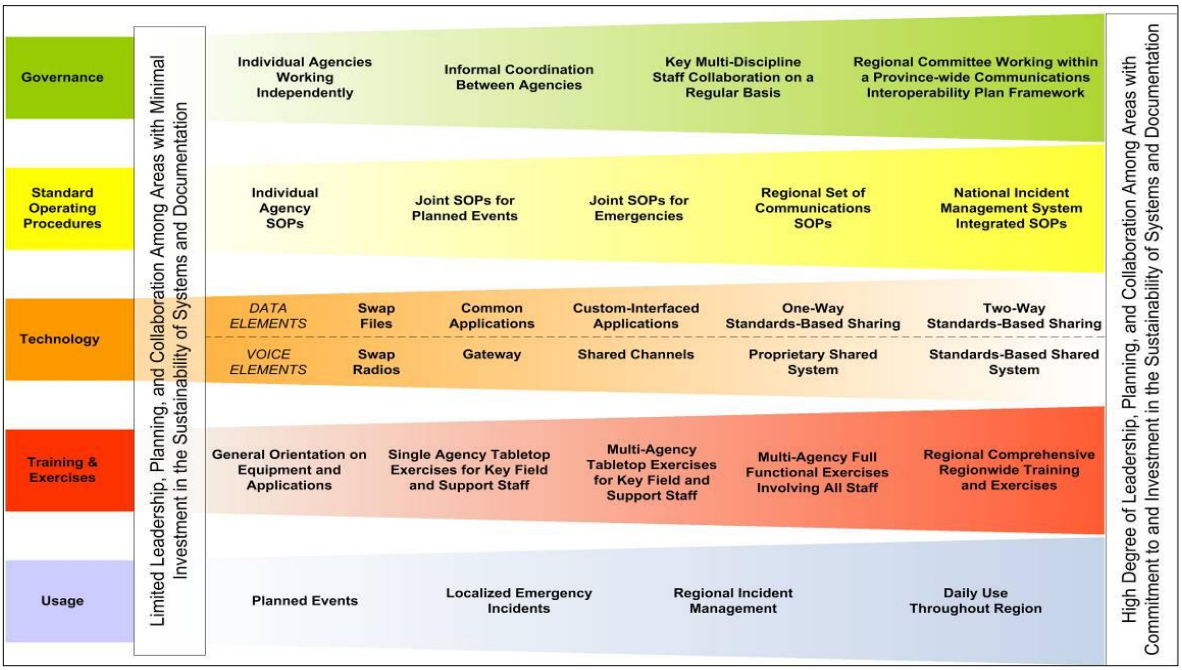
However, technology is not the biggest problem. Most public safety agencies agree that the technology issues are easy to deal with and address. The biggest challenges to interoperability are:

- Limited or fragmented funding
- Jurisdictional or chain-of-command conflicts in terms of equipment and procedures
- Availability of radio spectrum

With that in mind, CITIG has developed a visual tool based on five key criteria that public safety agencies can use to determine where they are on the road to interoperability (Figure 5). By using this tool, every agency can gauge the steps it needs to take towards full interoperability.

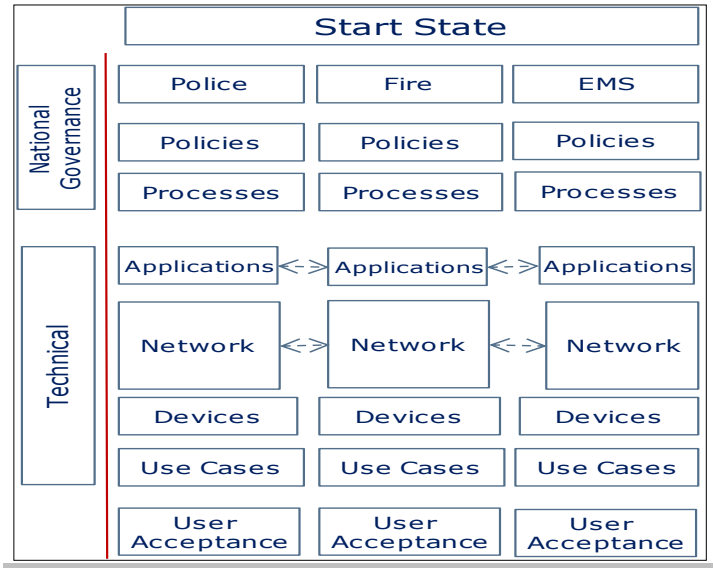
[1] SAFECOM, Office for Interoperability and Compatibility, United States Department of Homeland Security, www.safecomprogram.gov/about/Default.aspx.

Figure 5: The CITIG visual tool of the major stages towards full interoperability.



To reach the end goal and address the many challenges on the way, all agencies must work independently and together in a coordinated way. But, at the present time, each organization is working in a silo without any formal coordination between agencies (Figure 6). In addition, each public safety agency has made policy and technology purchasing decisions that make it difficult to enable full interoperability. Some, for example, have decided that communications systems will remain independent, despite the fact that in most cases radio transmissions from these organizations can be easily monitored by anyone with the right “off-the-shelf” equipment.

Figure 6: Public safety organizations are working in silos without any formal coordination between agencies.



As a result of this lack of coordination, public safety efforts in Canada are not as efficient and effective as they could be. That's because the intelligence gathering capabilities of the most important and critical resources of each agency — the people in the field — are not being used effectively.

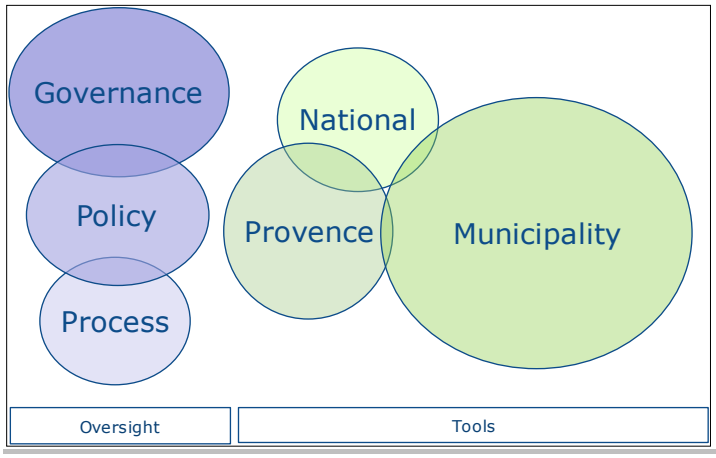
To be more effective, any technology solution proposed as a foundation for a national, wireless, interoperable public safety network must be built to leverage and complement the intelligence gathering capabilities of the feet on the ground in every agency and geography, and interact with every type of demographic. It should enable consolidation of that intelligence so that all agencies can work together to address any situation. Most importantly, it should leverage the best approaches of each agency, consolidate these best practices, and add analytics to enable all agencies to work seamlessly together at all times while drawing upon the same pool of data.

Governance oversight and technology interoperability can be separated in two categories as shown in Figure 6. The three main agencies can be seen in silo formation. Governance frameworks that dictate policies and polices that support processes are apparent in the governance oversight category. To execute requirements and policies efficiently, tools from technology can be used. As an overarching 'connector' national and regional applications transverse a network to support use cases and current processes for user acceptance by first responders.

In the start state, we see applications and networks switching between agencies, as they do today when responders swap radios as needed.

But current constructs come into play as governance is national, policies are provincial and processes are the responsibilities of the agency at a municipal level as it reflects regional crime patterns (Figure 7). Having the right level of governance and the right level of technology at the municipal, provincial, and national levels gives the right framework and oversight needed to put public safety on an evolutionary path. Finding the right mix will be a work in progress that will ensure interoperability and the overall vision is maintained.

Figure 7: Governance is national, policies are provincial and processes are the responsibilities of the agency at a municipal level as it reflects regional crime patterns.



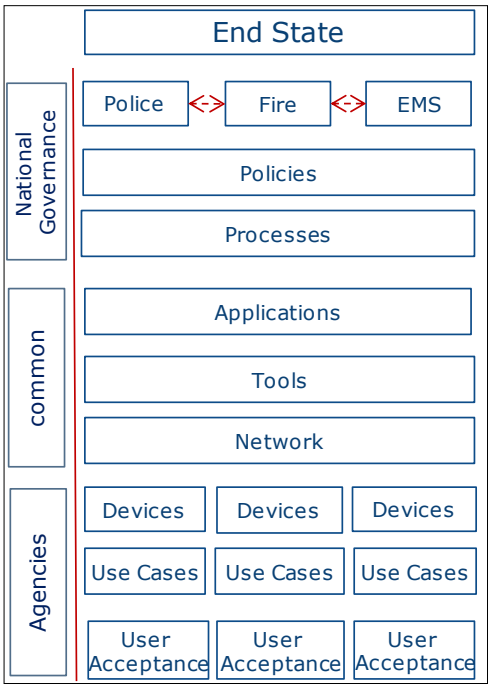
Moving Towards Interoperability

Public safety agencies want and need to work collaboratively. They know that interoperable communications networks will make their response to any emergency more effective. In fact, attendees at an EDGE® Innovation Event sponsored by General Dynamics Canada in 2012 identified six key points for consideration by all public safety stakeholders as they work towards developing a truly Canadian interoperable network solution:[2]

- Interoperability as a prerequisite for information sharing and efficiency by first responders
- The need for a system of systems
- The applications required to make personnel more efficient
- Hardware and software required to enable personnel to use the applications
- Efficient ways to get more information down the pipe to in-field personnel
- Efficient ways to enable interoperability with systems in the United States

But interoperability has to be applied in such a way that it enables each agency to continue to fulfill its mandate while addressing and implementing new technologies, applications and devices at its own pace. Therefore, the key to achieving the desired end state of effective interoperability (Figure 8) is to empower each agency to determine which technology will work best for its operations within the context of the ideal interoperable network solution. By approaching the process in this way, truly interoperable systems will be deployed by each agency.

Figure 8: The desired end state of effective interoperability.



[2] *"Public Safety Leadership Discussion: An EDGE Innovation Event"*, EDGE Innovation Network, April 2012.

Then, when a situation occurs, the networks, applications and devices will be in place to enable agencies to share information immediately by leveraging the most advanced technologies of the time.

Working towards interoperability with this type of cooperative structure will allow public safety agencies to create a network of networks, which will enable all agencies to jointly establish the most accurate situational awareness picture during any crisis. The architecture for this network of networks must be designed based on agreement on key governance and technology interoperability issues.

Figure 7 shows agency autonomy leveraging common resources for their responders and having the ability to interoperate as required at the agency level using a common communication language. Eventually new policies will be defined for agency interoperability nationally and for cross-border exchanges.

Addressing Policy as a First Step

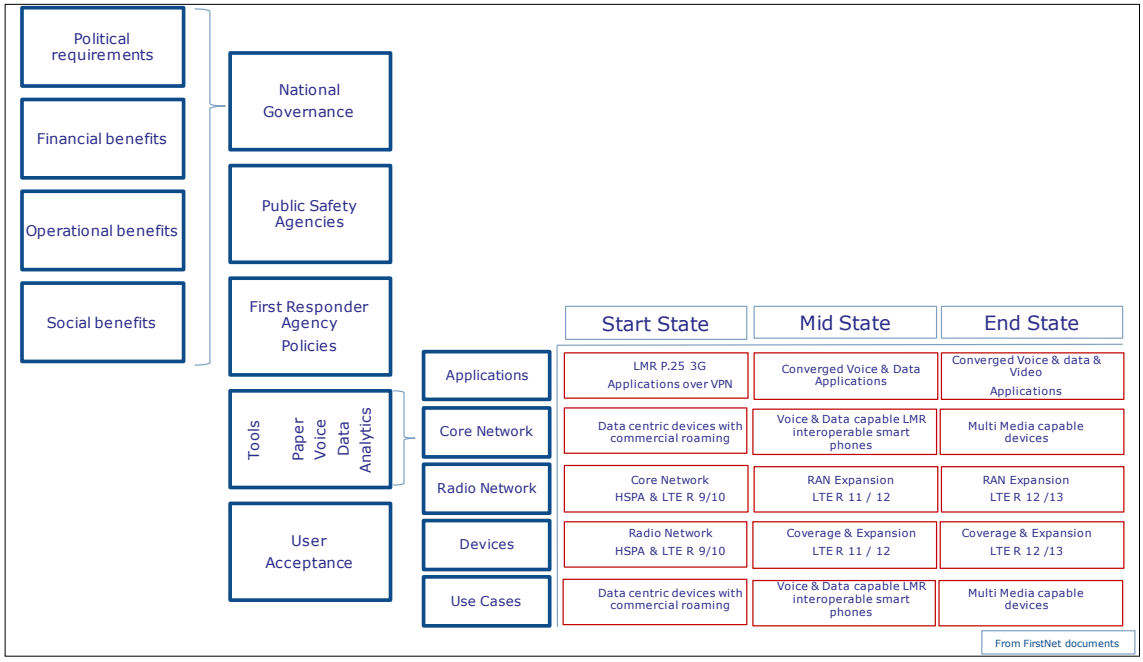
At the governance level, there must be agreement on how the network of networks will be used, who will have responsibility for national governance, and how governance will be determined at the local, regional and agency levels.

Several key questions must be dealt with to address this policy framework:

- What is the national governance requirement?
- Which metrics can be used to ensure value is delivered?
- How does that transfer to the various agencies?
- How does that governance translate into tools?
- How can we feed analytics into this model for all agencies?
- How does data transfer securely and in a compromised network?
- How can we evolve public safety on the same architecture?
- How can these tools be used most efficiently?

The answers to these types of questions start to collapse the silos into common technology, applications and devices for a more streamlined more manageable collection that can be deployed by all agencies (Figure 9).

Figure 9: Collapsing independent silos on the road to interoperability.



Current network and database consolidation programs developed by Shared Services Canada offer examples of how parts of this can be achieved. Movement in collapsing 43 federal government departments and agencies to a consolidated, efficient, secure system where common tools are leveraged is a key component. At the same time Shared Services has outlined its goal to move from more than 300 data centers to 20, and create a single, shared telecommunications network. This single effort is built on the idea of a technology foundation where tools are the enabler of interoperability, rather than the ultimate objective.

A similar approach by public safety organizations that maintains governance by all agencies will ensure that policies are respected and processes are followed. Governance interoperability across the agencies should be encouraged while ensuring management and user levels are simultaneously maintained. In this way, the management teams in each agency will be able to adopt new technology at their own pace, without having someone dictate the pace of integration.

Leveraging Existing Agency Investments

While governance interoperability is being developed, there must be agreement on the technologies that should be part of the interoperable network of networks.

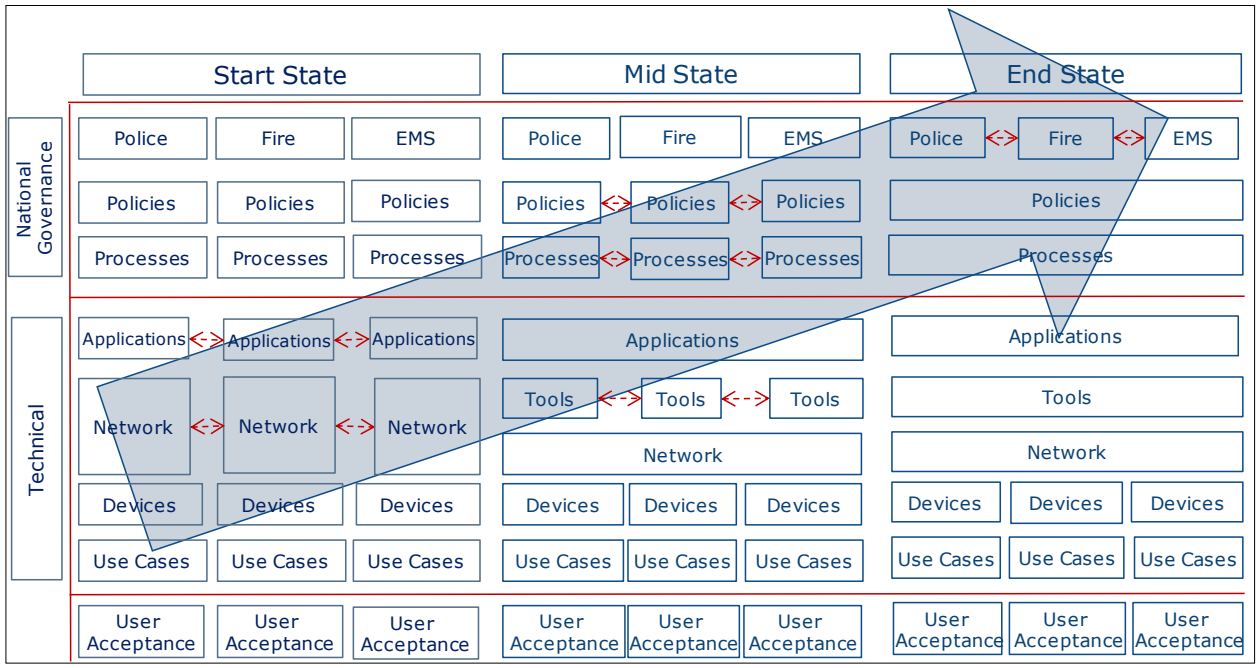
Currently, technology issues are being addressed by public safety agencies through several groups, including CITIG and CATA. Through these groups and others at the academic level, considerable steps have been made to consolidate the efforts of all public safety agencies to reach a common goal.

To support these activities, care must be focused on ensuring that legacy technology continues to interoperate and remains future compatible for as long as possible. This will allow all agencies to leverage their current investments in LMR, P25 and Wi-Fi systems, and adopt more advanced systems that extend the capabilities of existing networks and devices as they become available.

The eventual migration to an interoperable network infrastructure should allow all agencies to leverage the best of current technologies and end user devices, wherever possible. No technology should be left behind and all should be fully leveraged to enable the end goal. With this approach, there is no need for forklift upgrades. Everything should be evolved into a new infrastructure as required based upon function and need.

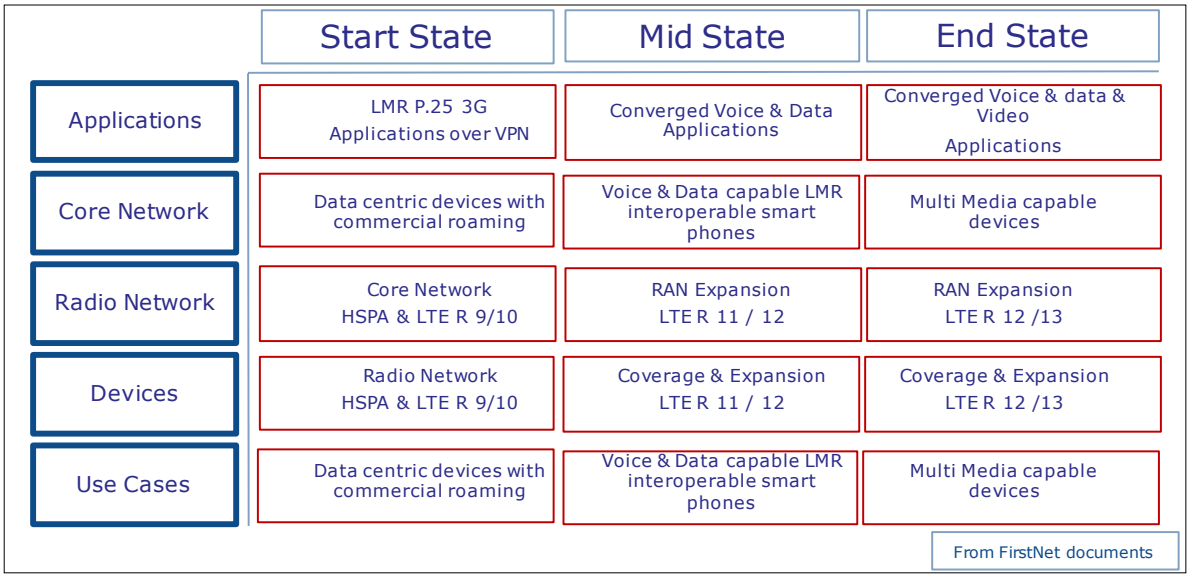
For example, if an agency only needs a narrowband radio today, it can select and deploy a narrowband radio that gives its personnel what they need immediately, but can also support broadband for tomorrow. This will allow each agency to go through a transitional phase — a mid-state — and a defined roadmap for full interoperability (Figure 10).

Figure 10: Evolving technology through a mid-state on the road to full interoperability.



As a result, all agencies across all municipalities in Canada will select their own regional tools at the right time in their evolutionary process (Figure 11) as they work towards full interoperability. National tools can be configured to operate within each agency's specific geographic region. These tools should draw from common databases of information to make their efforts more effective during joint, cross-agency operations where the other agencies would have different privileges to sensitive data.

Figure 11: Interoperability is enabled as agencies adopt tools at different stages in their evolutionary process.



Building a Test Bed Infrastructure

Moving towards the ideal end state can be accelerated by building comprehensive test bed networks that leverage existing independent infrastructures through a collaborative process between public safety agencies, industry, and academia. Together, all stakeholders can use the test bed to test, trial and tweak solutions for public safety and evolve solutions over time in a controlled environment.

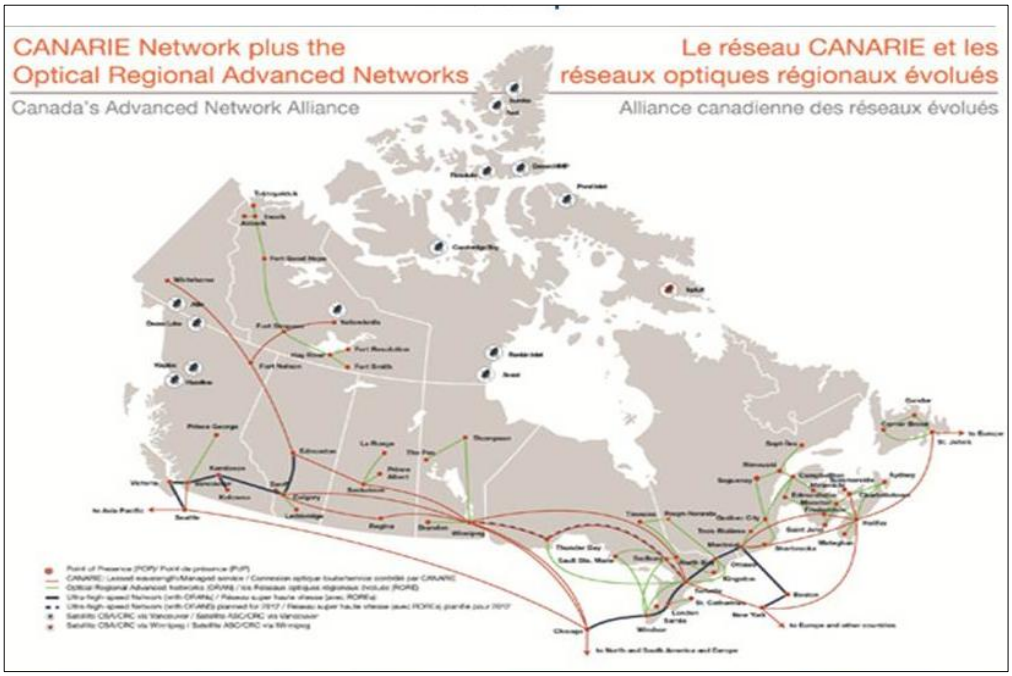
With this approach, industry stakeholders can provide the technology tools. Use cases from public safety agencies in Canada and the United States can provide the needed requirements for security and processes, while continually enabling refinement of the infrastructure requirements as a first step to creating the perfect criteria and the ideal interoperable network infrastructure. And academia can provide the non-biased review, analysis and recommendation of the tools and equipment needed to make this interoperable network effective for the long run.

With this collaborative approach, efforts can be focused on understanding the complex interoperability challenges that each agency faces, as well as how they can best be addressed by available and emerging technologies, such as LTE. Rather than creating everything from the ground up, or recreating something that already exists, thoughts should be focused upon how best to reinitialize existing infrastructure that is already in place. In this way, stakeholders can move quickly to use the test bed as a sandbox within which to integrate new technologies, applications, processes and devices, test them in a live controlled operational network environment, and possibly influence governance in terms of H2H, H2M, M2H, and M2M solutions.

Management of the test beds could fall into two categories. One managed and operated by a national organization, and the other managed regionally. Both must provide the right test bed environment, such

as that provided by the CANARIE (Figure 12) university network. Utility company infrastructures and backbone networks could intersect the national CANARIE network with province-wide networks and bridge industry and enterprise M2M sensors to public safety.

Figure 12: Two network test beds can act as sandboxes for public safety interoperability.



The CANARIE network is Canada's Advanced Research and Innovation Network. As one of the world's largest and fastest dedicated networks, it has over 19,000 km of fiber optic cable that connects over 1,100 academic institutes in Canada and provides access into the United States, Europe and Asia, as well as various research and innovation communities around the world.

The CANARIE network was created to ensure Canadians can engage in leading-edge research that requires much more capability and capacity than is available using the commercial Internet. CANARIE lets Canada's researchers, innovators and educators at all institutions across the country access massive data sets, sophisticated tools and complex scientific instruments for research and development in Canada and around the world.

Today, one million researchers, scientists and students at over 1,100 Canadian institutions, including universities, colleges, research institutes, hospitals, and government laboratories across Canada have access to CANARIE.

CANARIE offers an ideal sandbox in which to test the interoperability of the ideal public safety network, applications, devices, security, and analytical tools for predictive first response applications.

Understanding the Role of Technology

Where does technology fit in all this?

Obviously, technology is an enabler, and choosing the ideal network technology is one of the first steps in the development effort. By its nature, 4G Long Term Evolution (LTE) wireless broadband offers the most advanced network technology upon which to build an interoperable Canadian public safety network. It provides greater bandwidth, priority of service, better spectral efficiency, and the ability to work with a greater spectrum of devices moving forward. In addition, it offers the opportunity to leverage a large number of commercial level Application Programming Interfaces (APIs) that will allow developers to enable a variety of applications to interoperate and work smarter with analytical tools.

Going from the current state to the ideal end state requires a level of understanding from a test bed to leverage LTE and determine the best way to use the 700 MHz spectrum on a daily basis, in emergency situations, and in times of peace.

For daily use, there are many ways to optimize the network for a variety of public applications. One way is to allow public safety organizations to offer portions of the spectrum to other users when it is not in use for emergencies.

Of course, it is paramount that public safety organizations have priority in an emergency situation on all aspects of the network. Therefore, the end state network must be built with different levels of security and QoS at all levels to enable different national and regional public safety agencies to use a common infrastructure when and as needed. Analytical tools must also be built into the solution to enable command centers to analyze, collect and collate data and information during emergencies and take meaningful action on the data collected with API and Software Development Kits (SDKs).

Conclusion

First responders, devices, networks tools, applications, databases, clouds, processes, policies, accountability, governance, operations, finance, acceptance, analytics, security, systems, and networks, will all evolve at different rates for different agencies and for very different reasons. But interoperability is required by all agencies. The ideal solution must be flexible and agile, and robust enough to avoid potential failures.

By creating a sandbox environment that leverages the best practices of all agencies and the capabilities of advanced technologies, such as LTE, policy makers, public safety agencies, and the ultimate users of the final solution, in-field first responders, can work together to develop a truly Canadian interoperable public safety network.

But the timing of any effort is critical. If the available unused spectrum is not used, it could be reassigned for other applications. Therefore, the onus is on all public safety and security organizations to work together with industry and academia to develop a solution.

A task force approach that looks at governance and technology issues within the context of a test bed environment will have the most chance for success. It will facilitate the development of interoperability based on a network of networks that enables each agency to continue to fulfill its mandate while addressing and implementing new technologies, applications and devices at its own pace.

At the governance level, it will allow all stakeholders to agree on how the network of networks will be used, who will have responsibility for national governance, and how governance will be determined at the local, regional and agency levels.

At the technology level, it will allow efforts to be focused on ensuring that technology interoperability is legacy, current and future compatible. This will make it easier for all agencies to leverage their current investments in LMR, P25 and Wi-Fi systems, while seamlessly adopting more advanced systems that extend the capabilities of existing networks and devices.

Acronyms

Term	Definition
ATM	Automated Teller Machines
API	Application Programming Interface
CATA	Canadian Advanced Technology Alliance
CITIG	Canadian Interoperability Technology Interest Group
H2H	Human-to-Human
H2M	Human-to-machine
LMR	Land Mobile Radio
LTE	Long Term Evolution
M2H	machine-to-human
M2M	machine-to-machine
ROI	Return on Investment
SDK	Software Development Kit

Contacts

www.gdcanada.com
C4ISRSource@gdcanada.com

Subscribe to General Dynamics Canada's online C4ISR Resource Center for access to whitepapers, reports and information. You will receive bi-monthly updates by email.

Get instant access now: www.gdcanada.com/myC4ISR-Source