

It Won't Happen Here

Public Safety White Paper

Moving from narrowband to broadband communications



Abstract

Public safety and security incident management depends on legacy Land Mobile Radio (LMR) and limited data communication that can't meet the current need.

We can and must do better.



Executive Summary

Protecting the public and providing security is the primary role of governments at all levels. Whether it is routine police, fire, and paramedic operations, or being prepared to handle civil unrest, extremism, and natural disasters, first responders need reliable and secure communications and access to critical information that will save lives. But why expend scarce public safety resources on augmenting legacy narrow-band land mobile radio (LMR) technologies that originated in the 20th century, when modern wireless broadband technology has been around for more than a decade? As the complexity of global threats to our societies continues to increase, how long will governments allow this technology gap to continue?

Fortunately, this public safety capability gap is being challenged by the emergence of new, practical options for maintaining better situational awareness, mitigating the harm such events can cause, and for improving the effectiveness of public safety and security protective capabilities across the board. Building upon hard lessons learned in the past, jurisdictions at all levels have recognized the value of secure, dedicated-access, high-bandwidth public safety communication and data networks. Affordable, flexible systems running military-derived command and control applications are changing the game when it comes to emergency management and security preparedness around the world.

Having delivered secure, dedicated communication and information systems to military and security forces globally for more than 65 years, General Dynamics Mission System—Canada understands how to place the power of information in the hands of first responders and commanders. It is this experience and expertise that places the SHIELD Ecosystem at the forefront of this critical revolution in public safety and security – and makes it available for immediate service in a variety of easy-to-implement, easy-to-use configurations.



Contents

2	Public Safety Communications needs to Evolve
3	It Won't Happen Here
4	Don't Predict what might happen; Prepare for what will
5	Ready to Fight the Last War
5	The Limitations of legacy Land Mobile Radio (LMR) Systems
6-7	The Power of Information – The SHIELD brings reliability, security and Capability to public safety
8	Why use a dedicated network for SHIELD?
9	The Public Safety transition from narrow-band LMR to broadband LTE communications is gaining momentum



Public Safety Communications needs to Evolve

As global security conditions continue to evolve, governments at all levels are working diligently to provide the high-quality public safety voice communication, and data network capabilities needed by first responders. Particularly in urban areas, public safety and security officials have long recognized that reliable, secure communications are critical for responding to a wide range of potential threat scenarios. Regardless of whether it is routine security in areas where large numbers of people are going about their daily business, support to public events, or unexpected incidents of civil unrest, crime, violence, or natural disasters, public safety depends on the ability of authorities to rapidly develop, exchange, interpret, share and act on information. In many municipalities and even federal public safety agencies, the challenges of an expanding population base, urban density, geographic sprawl and the fragility and unreliability of commercial and public communication networks are hampering the critical task of civil protection.

In many jurisdictions, command and control of public safety services relies almost exclusively on traditional land mobile radio (LMR) systems, reporting to operations centers that often have only rudimentary ability to collate and interpret the incoming information. Voice and limited data connectivity over radio are hampering even routine operations, and when more complex situations arise, the ability of authorities to understand and direct what is going decreases rapidly. These limitations have prompted many jurisdictions to supplement their personnel with cellular phones to compensate for inadequate radio capacity and functionality. Relying on shared commercial cellular networks, even for backup communications, creates a security issue given the lack of assured, secure access to critical information. Furthermore, these shared networks can be quickly compromised by congestion or system failures. This creates a dangerous dependency on unprotected and fragile commercial systems that can't guard vital data. It can also lead to complacency among users and decision-makers that existing systems can be relied upon under crisis conditions, when they cannot.

In today's constrained fiscal environment, providing effective public safety and security requires working smarter, not harder. This means implementing secure, seamless, proven networks for accessing, sharing, and ultimately acting on information. It requires assured connections between senior decision-makers, operational commanders, and first responders on the ground. And it demands high-quality monitoring and situational awareness tools, running over controlled-access, dedicated, robust, high-bandwidth wireless data networks.

The technologies that support such systems exist, have been proven effective under military operational conditions, and are becoming available to the public safety and security sector. The availability of scalable, modular, turn-key wireless solutions means that even smaller jurisdictions can begin to address the need with integrated, full-spectrum capabilities that work out of the box. Beginning with modest up-front investments in areas of greatest priority, they can then grow their network and overall system capabilities as operational requirements demand, and fiscal circumstances permit.

It is an uncomfortable reality that today's average teenager with a smartphone can achieve equivalent or better situational awareness of developing public safety incidents than many front-line responders, locked into inefficient radio systems or reliant on commercial cellular services. But public safety cannot be left to ad-hoc command and control systems running on unsecure, unreliable networks - emergency management professionals need better tools. With security threats rising in probability, complexity and severity, it is no longer sufficient for governments to accept the limitations and known defects of legacy mobile radio and commercial cellular phone systems. Nor is it necessary.

It Won't Happen Here

On October 22, 2014, at 9:50 a.m., in the morning, a lone gunman approached the Canadian National War Memorial in downtown Ottawa with an unrestricted, lever-action hunting rifle, and proceeded to fatally shoot one of the unarmed military ceremonial guards. He then drove to the Parliament buildings, burst through the main entry, and ran down the Hall of Honour towards the Library of Parliament. Before being shot moments later by the responding RCMP tactical team, House of Commons constables and the Parliamentary Sergeant-At-Arms, he passed mere meters from committee rooms where the Prime Minister and Leader of the Opposition were conducting business.

The “active shooter” phase of this incident took place in less than 15 minutes from the moment the first shot was fired, to when the assailant was confirmed deceased.

Unfortunately, because the authorities on-scene and in the many surrounding dispatch and command centres could not communicate effectively with each other to establish a trusted, coherent picture of the situation, a significant portion of the Ottawa downtown core was shut down for nearly 10 hours. In the confusion, hundreds of government offices and businesses were locked down and all five bridges connecting Ottawa with neighboring Gatineau were closed, along with 19 schools. An estimated 80,000 residents and commuters were directly impacted by movement restrictions as authorities tried to confirm first whether there had been more than one attacker, and then worked to secure other public spaces as follow-on reports of suspicious sightings began to stream in. It is estimated that more than 300 first responders from the RCMP, Ottawa Police, House of Commons Security Service and Senate Protective Services were involved, in addition to large numbers of fire and paramedic personnel that were directed to an unfolding, highly chaotic scene.

An independent review of the Parliament Hill attack was conducted and not surprisingly, almost all aspects related to command and control of the incident were completely deficient. This included poor or non-existent communications among the agencies involved at all levels, an inability to receive, triage, analyze, and integrate emerging information to permit effective decision-making, and lack of a common operating picture or the means to share it via reliable, secure communications and data network.


As Parliamentary Guards stationed at the East Block observed the attacker running towards the Peace Tower, they were unable to inform the RCMP stationed there, because their radios were incompatible. Nor could they or the RCMP communicate with the Ottawa Police converging on the War Memorial, who were using yet another legacy system. Within the building, members of other protective organizations using the same radios were on different channels – and had neither the time nor the system to activate a coordinated communication plan into action in the heat of the developing attack and subsequent gunfire. Even among fire and paramedic responders, the operational limitations of voice radio networks were evident: as transcripts show, simply organizing the dispatch response to the initial report of a person shot at the War Memorial took more than two minutes, involved at least five different parties on a single voice circuit, and three channel changes – and this was before communications spiralled into incoherence.

“ Alternate forms of communicating need to be explored... Text messaging caused as much saturation as voice communications.

Parliament Attack After-action review, Government Operations Centre / Shared Services Canada, October 2014

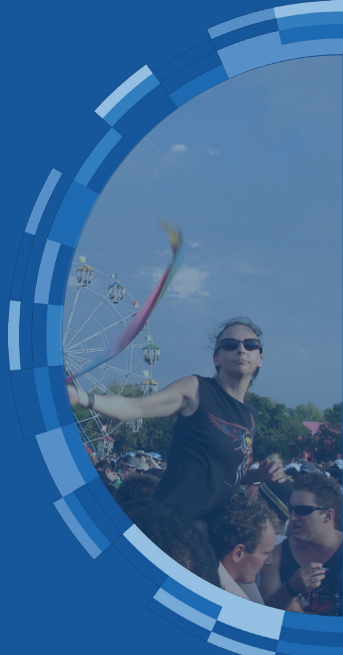
“ Having timely and accurate information is very important. It determines how we respond, whether it's going to be urgent lights and sirens or it's going to be a routine response, normal driving conditions, and how many units are going to go to the call... It makes a big difference; it changes the entire dynamic of the call.

Deputy Jesse Trebelik - Senior Deputy, Adams County Sheriff's Department




Don't Predict what might happen; Prepare for what will

When considering how best to allocate scarce resources between public safety and security requirements, and other, equally pressing social spending priorities, government officials responsible for risk management often rely on models that attempt to assess the probability of adverse events, and project the likely severity of their impact. Senior public safety leaders will argue that being prepared for all eventualities is not only more important, but more prudent. The logic of human decision-making can be paradoxical: if an event is inherently unpredictable, and the adverse impact seemingly unavoidable, individuals and organizations alike tend to devalue or ignore the potentially positive effects of mitigating approaches – even when very real advantages can accrue, with modest effort. It's as if the sensationalistic quality of such dire public safety events cause us to figuratively throw up our hands – after all, if there is no practical way to address the problem, we may as well carry on with the mostly-adequate capabilities already in place.



This is a critical leap of logic when comparing the wholly-inadequate capabilities of legacy voice and voice + limited data systems with the disruptive advantage of secure, dedicated public safety broadband wireless networks. While neither legacy nor new approaches will affect the probability of a critical incident, only a well-implemented public safety broadband network will reliably empower first responders with access to life-saving tools and sensors, while giving commanders on the ground the information needed to make key decisions to protect the public.

Public safety agencies around the world routinely produce after-action reports related to large scale public events, complex attacks or natural disasters. A common lesson identified is communications – as soon as more than five parties try to use a single radio net, multiple voice reports begin streaming in to a command post, or thousands of people start texting at the same time there is a 100% chance of first responder miscommunication, confusion, data slowdown, complete network failure and eventually command and control breakdown. After-action analysis in critical incident locations such as Brussels, Sydney, Paris and more recently Barcelona repeatedly show that legacy communications approaches failed first responders when they needed it the most. These radio limitations and shared network dependencies can also affect routine events and celebrations, where the challenge of crowd control and traffic management are exacerbated by narrowband, voice-centric radio systems that prevented agencies on the ground from seeing the big picture, or reacting quickly enough to prevent bottlenecks and security jams.



Put another way, while any number of terrible incidents MAY occur (albeit with very low probability), it is virtually certain that significant command and control breakdowns WILL happen – wherever and whenever complex public safety incidents or major events force first responders and their leadership to rely on legacy LMR systems, even when supplemented by commercial cellular networks.

Ready to Fight the Last War

Among Western militaries, considerable effort is expended when specifying and procuring weapon and sensor systems to ensure that the capabilities being introduced into service are the ones most likely to actually be required (and useful) in battle.

The danger that must be avoided at all costs is “preparing to fight the last war;” that is, sticking with what is comfortable and proven effective in the past, when the nature of the threat has changed in ways that significantly if not fatally reduces the effectiveness of the existing legacy approach. An example would be the development of air defence radars in the Second World War, which gave defensive forces the actionable information and the “big picture” awareness they needed to respond to a quantifiable and imminent threat, as opposed to waiting for multiple human observers to relay enemy sightings by voice, which invariably left little time to dispatch response forces.

This analogy can be used to in the public safety environment where legacy radio reporting only gives a verbal interpretation of an event as opposed to receiving critical information in near real time such as personnel location, data and video that can be collected from responders and sensors in the field using a dedicated high-speed network to rapidly collate simultaneous inputs into a common operating picture for informed decision making.

The Limitations of legacy Land Mobile Radio (LMR) Systems

In the public safety domain, the dominance of LMR and limited-data LMR (even when used in conjunction with commercial cellular networks) is ending, as these technologies are nearing a similar point of functional obsolescence. To be clear, this is not related to any fundamental technical defect in traditional, point-to-point radio communications: push-to-talk functionality and simple-to-use voice communications devices will, in the near-term, continue to have a place in public safety operations.

Primary shortfalls of the current patchwork of imperfectly integrated LMR and LMR + civilian cellular include:

Insufficient Capability – During large scale events, or when a complex incident occurs, such as one with multiple simultaneous locations, rapid changes in the geographic position of the area of interest, or cascading effects that required detailed, time-sensitive knowledge to assess, voice communications systems quickly become overloaded and situational awareness is lost. There are fundamental limits on the ability of public safety personnel using conventional voice reporting systems to accept inputs, assess their relevance, enter the information into a situational awareness tool, render decisions, issue command direction, and then monitor the outcome. The overriding requirement to protect lives imposes an equivalent demand on public safety leadership to build and manage a common operating picture. This simply cannot be done effectively for complex incidents using systems built around voice reporting.

Unsecure and Vulnerable to Exploitation – Low-grade or non-existent encryption of narrowband land mobile radio systems (LMR) and shared commercial broadband cellular networks raises the risk of information being monitored, compromised or stolen. From readily available police-band scanners to more sophisticated tools for cellular monitoring and even decryption, the primary point of tactical vulnerability in many public safety response systems remains the communications links between front-line personnel and leadership. Add to this the fact that several international commercial network providers are quietly listening to all their client traffic through backdoors and remote servers. New technologies include automated systems that collect, digitize, and rebroadcast LMR transmissions via cellular phone applications, allowing criminal or terrorist actors to exploit near-real-time access to public safety and security information as incidents unfold. For example, during the 2008 terrorist attack in Mumbai, India, assailants used Voice-over IP (VoIP) techniques to transmit instructions and maintain situational awareness, in some cases using spotters on-scene and civilian television feeds as sources of information.

Authorities were aware of the activity, but faced the difficult choice of bringing down the civilian cellular phone infrastructure – which they themselves were using for command and control – or continuing to allow the terrorists to direct operations over an active network. Existing legacy networks, regardless of whether they are voice-only radio or cellular data, have become a prime point of security vulnerability for public safety and security organizations.

A lack of resilience – The primary drawback to the overall resilience of commercial cellular networks is the fact that when emergency situations arise, network capacity is often overwhelmed by the sudden spike in demand. During the attack on the Boston Marathon, every major cell phone carrier's service in the region rapidly became overloaded. After the 2014 San Francisco earthquake, network use jumped up to 800%, preventing voice and data communications among civilians and first responders alike. Even when the physical network is undamaged, the inability of public safety services to quickly control access means that under emergency conditions, the civilian cellular system is effectively denied to their use.

Of course, network resilience can also be affected physically. While some portions of the civilian cellular network have limited backup systems to preserve accessibility during power interruptions, these cannot be relied upon to provide full coverage under all circumstances.

General Dynamics and First Net

General Dynamics is a key member of the FirstNet team led by AT&T, which will design, develop and deliver the United States' Nationwide Public Safety Broadband Network.

The Power of Information – The SHIELD brings reliability, security and Capability to public safety

In contrast with the untidy kludge of LMR-based systems that attempt to connect first responders across multiple operational organizations and functional domains, The SHIELD eliminates communication challenges with a system architecture that integrates legacy systems and sensors with modern smart devices and data fusion interfaces to optimize operational effectiveness and facilitate interoperability with multiple public safety agencies. The SHIELD ecosystem is an integrated suite of networked hardware, sensors, and user interface devices operating on a robust, secure and dedicated, 4G/LTE network. Along with software applications, including geo-location, texting, video sharing and role-specific decision aids, the SHIELD system provides dedicated, high-reliability, secure voice and data access capabilities to public safety and security first responders, scene of action commanders, and command centers.

The network backbone of the ecosystem is government-owned, adheres to the 4G-LTE specification, and operates on multiple bands. Depending on the installation and operational requirements, SHIELD systems can interoperate with traditional land mobile radio (LMR) systems, which allows agencies to transition from LMR to LTE at their own pace. The SHIELD involves a mix of commercial and ruggedized, military-grade components with layered encryption, and cyber-protection capabilities to address the mission-critical requirements of the public safety and security role in a way that can't be matched by traditional voice-only or voice + limited data systems.



The SHIELD ecosystem comprises four distinct network communication capability packages, each of which is optimized for a different role:

EmergencySHIELD – A rapidly deployable 4G-LTE data communications network and supporting operations capability for emergency response to a security situation or disaster relief. Configurations include “network in a box” and/or “cell on wheels” (COW) systems, integrated with ruggedized distributable handsets and “command post in a box” capability, to allow a secure, dedicated 4G-LTE network to be quickly established under austere or adverse conditions, and to provide first responders with secure, controlled-access, smartphone-based, easy-to-use hardware and applications to support situational assessment, command and control, and a wide range of safety/security response activities.



CitySHIELD – A combination of mobile (vehicle-mounted) and fixed 4G-LTE data communications networks optimized for persistent public safety and security use in large, geographically diverse, densely populated urban areas. Including network infrastructure, configurations consist of a mix of ruggedized smartphones, headset/handset arrangements, and other handheld or vehicle mounted interface devices (tablets and/or laptops), mobile and fixed command post installations, relocatable net-enabled cameras, and necessary interfaces to legacy systems that support public safety, including existing LMR systems, traffic monitoring cameras, and public safety and law enforcement databases. CitySHIELD supports all traditional operations and dispatch functions, and adds computer-aided dispatch, resource tracking, intelligence sharing, evidence collection, license plate recognition, mapping and location tracking, web intelligence gathering, biometric facial recognition, and all standard IP-type telephony services including push-to-talk capability.

InfrastructureSHIELD – A specialized sensor implementation intended to be integrated, and optimized to protect buildings, geographical locations, or critical infrastructure. Key additional configuration options include fixed and mobile electro-optical sensors, fiber optic warning/detection equipment, underwater and underground sensors, radars and UAV detection systems, and airborne sensor inputs from UAVs or aerostats. Other functionalities over the standard City SHIELD offering include training and simulation modes, fixed-location remote sensor controls and operations management functionality, as well as physical and network access control and monitoring capabilities.




BorderSHIELD – A specialized 4G-LTE network and sensor implementation optimized for tripwire and area monitoring over large, austere, geographically diverse areas where supporting power and service infrastructure is limited or lacking altogether. As with the Infrastructure SHIELD offering, configuration options include fixed and mobile electro-optical sensors, fiber optic warning/detection equipment, underwater and underground sensors, radars and UAV detection systems, and airborne sensor inputs from UAVs or aerostats – along with training and simulation capabilities to allow operational assessment. However, Border SHIELD also adds austere power generation, options for vehicle-mounted management and control of sensors, mobile command post capabilities, and (if required) over-the horizon communications monitoring and satellite data interface options as well as other non-4G wireless data exchange options, to maintain continuity of surveillance in extremely remote areas.



Why use a dedicated network for SHIELD?


With the prevalence and easy accessibility of commercial cellular networks and hardware, the advantages of and requirement for parallel 4G-LTE networks dedicated to public safety and security functions may not be clear. Given the importance of the public safety function, unless they are government-owned and operated, the voice and data communication networks in question can never be fully optimized, or secured to deliver the following mission-essential capabilities:



Reliability – Unlike commercially-provided and managed cellular networks, the core SHIELD components and infrastructure are built to military standards to ensure guaranteed uptime even under difficult conditions, and configured to optimize the reliability and security of public safety communications and data exchange between all network elements. This includes not only user display/interface devices such as phones, tablets and laptops, but also transmit/receive nodes, servers, cameras and other IP-enabled sensors, applications, and fixed and mobile terminals. When SHIELD is needed, it is there.

Security – By restricting vital public safety and security information to dedicated, encrypted SHIELD networks owned by the user governments or organizations, authorities can be confident that operationally and legally sensitive information is accessible to only those with a need to know, protected from unauthorized use, and archived securely for post-action analysis and judicial examination. This includes additional layers of security on top of the existing 3rd Generation Partnership Project (3GPP) LTE security architecture, including advanced user and device authentication, and Internet Protocol Security (IPSEC) confidentiality. SHIELD is protected by design against foreign network operators, criminal elements, or other cyber-entities.

Functionality – The curated, certified mission-critical SHIELD application suite ensures the right information and key functionalities are available to first responders, scene of action commanders, and command center authorities alike. This includes voice and text services, persistent as well as push and pull access to geographic locations of vehicles, public safety personnel, and identification databases, relevant maps and infrastructure diagrams, medical information, unit operational status and logistics requirements, external data from monitoring equipment such as fixed cameras or UAVs, event/incident reporting, and automated decision-assistance tools. SHIELD offers a powerful, easy-to-use command and control toolset based on systems proven effective in military and specialized security environments.



Flexibility – SHIELD offers a variety of fixed and mobile network options that can be used continuously for routine operations, or rapidly brought on line in emergencies, according to need and cost. Because of its rugged, military-specification design and focus on ease of use under austere or adverse conditions, network equipment can be readied for operations quickly, and sustained in the field with limited training. Additional users, nodes, vehicles, and sensors can be seamlessly integrated into the network in real time using military mesh network technologies, and the system automatically adapts to radio interference and even jamming conditions, when they are encountered. Regardless of the mission, there is a SHIELD configuration that can meet the need.

The Public Safety transition from narrow-band LMR to broadband LTE communications is gaining momentum

An increasing number of international governments, including the US, UK, Canada, South Korea and Australia have begun the transition to public safety broadband communications. The Government of Canada recently announced its intent to pursue a Canadian Public Safety Broadband (PSBN) capability, and has created a dedicated team including representatives from Public Safety Canada, the Department of Innovation, Science and Economic Development Canada (ISED), and Defence Research and Development Canada's Centre for Security Science (DRDC CSS).

While this organization has indicated it will solicit inputs from government stakeholders, as well as the telecommunications industry and academia, General Dynamics believes that as a globally-recognized military systems integration and communications provider, it has the experience and technology to kick-start the process of building operational PSBN capability for Canadian and international public safety users now.

Cost and technology considerations dictate that there will still be a role for LMR and voice-centric operations in the foreseeable future, at least until LTE push-to-talk capabilities can provide the full range of mission-critical communications capabilities required. However, in the face of growing public safety and security needs, the massive qualitative

advantages of SHIELD communications and data network capabilities – including enhanced situational awareness, geolocation of personnel and mobile units, assured and secure voice and data communications, sensor integration, and advanced decision-support tools – make delaying the transition a perilous and unwise choice.

With modest initial investments that can grow and scale as demand and capability increase, dedicated SHIELD network communications solutions are an important complement to (and interoperable with) existing LMR suites. Legacy systems such as P25 have already reached or are reaching their limits of data capacity, are increasing in cost every year, and suffer from fundamental shortfalls when they must be relied upon for command and control in complex emergency situations. By contrast, advanced 4G and emerging 5G technologies are dropping in cost as competition and other market forces such as open standards encourage innovation. When combined with General Dynamics' military-grade design pedigree, affordable smart devices, and the end-to-end SHIELD focus on security and ease of operation for both hardware and applications, creating highly effective, dedicated public safety networks in either fixed or mobile configurations doesn't require more consultation – it only takes the will to do so.

After all, in the challenging global security and public safety environment facing governments today and in the future, the wisest and most cost-effective way to respond to the possibility of critical incidents is not to try to predict whether they will occur - but to make meaningful investments in the systems and capabilities necessary to mitigate their effects, when they inevitably happen. The time to begin the migration from legacy LMR systems to true 4G-LTE public safety infrastructure is now.

General Dynamics and the BRIC

The Bridging Research and Interoperability Centre is a public safety technology development initiative run by the University of Regina.

