NIST Technical Note 1917

Public Safety Analytics R&D Roadmap

Ryan Felts
Marc Leh
Tracy McElvaney

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.TN.1917

National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Technical Note 1917

Public Safety Analytics R&D Roadmap

Ryan Felts
Corner Alliance
Washington DC

Marc Leh
Corner Alliance
Washington DC

Tracy McElvaney
Public Safety Communications Research Division
Advanced Communications Research Group

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.TN.1917

April 2016

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

National Institute of Standards and Technology Technical Note 1917
Natl. Inst. Stand. Technol. Tech. Note 1917, 78 pages (April 2016)
CODEN: NTNOEF

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.TN.1917

Public Safety Analytics R&D Roadmap

CTL Communications Technology Laboratory

PSCR Public Safety Communications Research

U.S. Department of Commerce – Boulder Laboratories

Copyright:

Disclaimer:

The names of certain commercial products and manufacturers have been fully disclosed in this document in order to provide the reader with a maximum amount of information. This should not be construed in any way as an endorsement of these products by NIST; other products will work equally well or better.

Table of Contents

Public Safety Communications Research (PSCR) Program
Public Safety Analytics R&D Roadmap Report

Executive Summary

The public safety community is in a period of great transition. Over the next 20 years, technology advancements will increase accessibility of data/video applications to public safety, and allow for the eventual migration of voice communications from disparate Land Mobile Radio (LMR) networks to a nationwide Long Term Evolution (LTE) broadband network, the Nationwide Public Safety Broadband Network (NPSBN). Emerging technologies within this new infrastructure present opportunities and challenges for public safety, and the process of modernizing responder communications requires significant coordination and planning. To facilitate the transition from LMR to LTE, the Public Safety Communications Research (PSCR) program initiated a research and development (R&D) planning process to determine what technology investments are of highest priority to the public safety community.

The *Public Safety Analytics R&D Roadmap* is the second in a series of technology roadmaps that PSCR will develop over the next few years to better inform the investment decisions of R&D organizations supporting the public safety community. This document aims to assist in planning for public safety communications research and optimize the allocation of the $300 million apportioned to NIST from the Middle Class Tax Relief and Job Creation Act of 2012. The NIST R&D funds were raised from the AWS-3 spectrum auction, which concluded in January 2015. This report intends to outline the current state of analytics technologies, forecast the evolution of analytics capabilities and gaps, and identify potential R&D opportunities that would improve public safety's use of data analytics within operational settings. After conducting additional roadmaps in other priority technology areas, PSCR will identify the R&D project ideas that pose the greatest operational benefit to public safety and prioritize its Public Safety R&D program accordingly. Given the scope of technology under consideration and level of effort required to deliver enhanced data analytics to public safety, PSCR hopes that these findings and recommendations will not only address technical barriers to adoption and accelerate innovation, but also provide opportunities to engage and inform stakeholders across all levels of government, industry, and academia.

The roadmap was drafted by soliciting input from technology experts, end-users, and researchers across government, public safety, industry, and academia. This cross-disciplinary approach enabled PSCR to evaluate existing R&D efforts, potential partnerships, and future projects against public safety's unique set of priorities, requirements, and long-term goals. After reading this report, organizations will understand:

- The trends and drivers affecting public safety, public safety broadband, and the analytics technology domain.
- The projected evolution of analytics software, applications, devices and networks over the next 20 years.
- The enabled operational capabilities that public safety stands to gain by adopting the forecasted analytics technology capabilities.
- The enabling actions and actors that are driving the evolution of analytics technologies.
- Gaps and Barriers that need to be addressed before analytics can fully benefit public safety operations.
- Potential R&D opportunities that would complement existing analytics efforts and help transform this technology area into an asset for public safety operations.

Roadmap Approach and Framework

PSCR has organized the *Public Safety Analytics R&D Roadmap* report into three main sections: Software & Applications, Devices, and Networks. Within each of these technology categories, PSCR discusses several operational objectives that surfaced as natural themes from the Analytics Working Group's collective input. These Operational Objectives, as shown in Table 1, are defined as feasible, impactful project areas that R&D investment targeted to analytics could deliver to the public safety community. These outcomes would allow public safety to fulfill its mission more efficiently and effectively. The Operational Objectives enabled by analytics discussed in this report include:

Report Section	Operational Objective
Software & Applications	Integration of Multiple Data Sources
	Improvement in Data Processing Capabilities
Devices	Devices serve to create, collect, store, process, and transmit data
	Devices as communications infrastructure
Networks	Network Self-Optimization
	Decentralization of Networks

Table 1: Public Safety Analytics R&D Roadmap Operational Objectives

To scope this report, the working group's input relating to Analytics Technology Capabilities & Gaps, Enabling Actions & Actors, and Enabled Operational Capabilities are embedded as supporting sections within the Operational Objectives. The report lists potential R&D opportunities relating to each Operational Objective.

Recommended Public Safety R&D Opportunities

Table 2 highlights a more extensive list of R&D Opportunities discussed in this report, which were identified by the Public Safety Analytics Working Group for the public safety R&D community to consider. These were identified within the context of environmental trends and drivers, anticipated technology evolution, and projects being pursued outside of the public safety space so that PSCR and other interested R&D organizations could complement – rather than duplicate – ongoing efforts in the broader analytics technology sector. These R&D project ideas are not intended to be an exhaustive list of the ways in which analytics technology needs to improve to better serve public safety. Rather, PSCR hopes that the readers of this report will recognize these opportunities as initial steps that would help make analytics more operationally viable for the public safety community.

Report Section	Recommended Public Safety R&D Opportunities
Software & Applications	Develop a software development guide on how to integrate externally available data sources with public safety-owned databases.
	Create a national, regional, or statewide "Information Sharing and Analysis Center" specifically for public safety use. The platform could operate similarly to data.gov but with public safety security and authentication requirements.
	Perform a gap analysis between disparate databases public safety projects to use to identify the compatibility errors and degree of inconsistency or inaccuracy incurred when merging these datasets. Estimate the time and cost required to resolve data integrity issues.
	Conduct pilot programs for commercially available data integration platforms in public safety settings and provide feedback on improvements to vendors and public safety end-users.
	Establish a software analytics framework to integrate disparate data sources.
	Define common "Public Safety Internet of Things" data standards and processing models for specific public safety support activities.
	Develop software analytics standards-based framework to integrate and process disparate data sources.
	Partner with R&D community to design tools that analyze physical attributes and multimodal biometrics in images.
	Pilot test programs that use querying languages to process real-time data streams.
Devices	Explore using device-embedded analytics to better manage (prioritization, bandwidth use, etc.).
	Define requirements (data processing, security, storage, etc.) for on-device recording and storing of communications transcripts.
	Review advances in ultra-low size, weight, and power (SWaP) Evolved Packet Core (EPC) and eNodeB technologies for wearable LTE devices.
	Develop an analytics framework for integrating disparate data sources across public safety devices and 3rd-party devices and sensors.
	Define minimal user requirements, including security requirements, for responder-worn sensors and computing power needed to deliver on these requirements. Explore new low power Internet of Things security algorithms.
	Define data standards and exchange protocols for public safety-worn sensors.
Networks	Develop network resiliency and prioritization services to enable mission-critical data when the network goes down or is overloaded from a bandwidth standpoint.
	Development of a network-based element that discovers critical pieces of content needed from disparate data sources across the public safety enterprise, and delivers them to public safety users. Create a standard and/or usage scenario that indicates what information or analytical capabilities are necessary during routine (house fire, vehicle crash, etc.) and extraordinary events (forest fire, flood, etc).
	Investigate modularization of network components that serve multiple purposes for the use of creating resilient mesh networks.
	Explore constructive interference R&D to maximize spectrum usage and limit harmful interference.

Table 2: Recommended Public Safety R&D Opportunities

Conclusion

In addition to providing context and recommendations for future R&D investment, the report discusses PSCR's process of designing the Public Safety Analytics R&D Roadmap, its stakeholder involvement strategy, and other priority areas that could become the subject of future technology roadmaps. For more information, please contact PSCR Division Chief Dereck Orr (dereck.orr@nist.gov), or PSCR support staff Ryan Felts (rfelts@corneralliance.com) and Marc Leh (mleh@corneralliance.com).

Purpose

Over the next 20 years, the public safety community will simultaneously face unprecedented challenges and be presented with paradigm-shifting technologies. In the face of these challenges and opportunities, the Public Safety Communications Research (PSCR) program initiated a deliberate research and development (R&D) planning effort in 2013 to determine what technology R&D investments are necessary to transition public safety data, video, and eventually voice communications from the Land Mobile Radio (LMR) environment to a nationwide Long Term Evolution (LTE) broadband network. In order to optimize its investment resources, PSCR solicited input from first responders, officials from all levels of government, industry leaders, and academia. By leveraging expertise from across its diverse stakeholder base, PSCR can more accurately map the current state of the public safety and communications industries identify current and future technology gaps, and make better-informed decisions on where its R&D initiatives will create the greatest impact.

Analytics is the second in a series of technology roadmaps PSCR will develop over the next few years. PSCR initiated its R&D Program by publishing a Location-Based Services roadmap in Spring 2015 and has followed a similar process in developing this Public Safety Analytics R&D Roadmap Report. Analytics was selected by PSCR as an important R&D opportunity area because it demonstrated high leveragability, feasibility, impact, and return on investment to the public safety community. It also continues to receive tremendous attention from technology companies, universities, and other government organizations, which underscores the importance of systematically surveying and recommending investment opportunities in the data analytics sector. Data Analytics is a vast subject area, so in order to optimize the allocation of public safety's R&D resources, PSCR will need to continue to engage stakeholders, coordinate activities, and create an understanding of the various actors advancing analytics technologies. After conducting the Analytics and other roadmaps, PSCR will proceed to identify, prioritize, and launch formal R&D projects.

Intended Roadmap Audiences

While PSCR has undertaken the process to create this Public Safety Analytics R&D Roadmap, PSCR is not the sole intended audience for this report. The level of effort, resources, and capabilities needed to deliver improved analytics capabilities to the public safety community, both in the short- and long-term, are well beyond the scope of PSCR's ability to address alone. Therefore, this roadmap is intended to inform other R&D efforts undertaken at the federal level as well as within industry at large and the academic community. This report is also intended to educate decision-makers at the federal, state, and local levels as well as the public safety community about the capabilities that analytics may provide in the future and actionable initiatives that would help bring about improved analytical capabilities in public safety (Fig. 1).

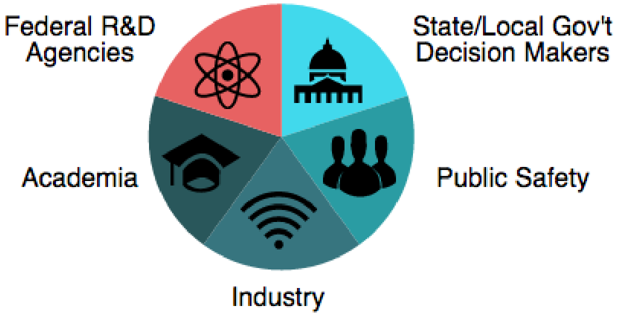


Figure 1: Intended Audiences of the PSCR Public Safety Analytics R&D Roadmap

Roadmap Design Principles

The following principles have guided the process as PSCR created the Public Safety Analytics R&D Roadmap:

- Build a vision of where the public safety community wants to go, determine what technologies are needed to get there, and provide a route for achieving the vision.
- Make R&D decisions based on priorities set by the public safety community.
- Assume that public safety might have to adjust operations to fully realize the benefits of new technology.
- Leverage ongoing efforts by other partners to develop and implement the roadmap. This approach will allow PSCR to focus resources to complement and not duplicate ongoing efforts.
- Get far enough ahead of the technology development curve to influence commercial R&D and leverage economies of scale.
- Enable public safety to meet generational and public expectations.
- Employ a cross-disciplinary approach to gather input and develop R&D plans for PSCR initiatives.

Building on Location-Based Services:

Initial research into the design of a roadmap framework for PSCR's R&D efforts took place in 2013 and 2014. In addition, PSCR incorporated several lessons learned from the Location-Based Services Roadmapping process into the development of the Public Safety Analytics R&D Roadmap. Some of the lessons learned that influenced PSCR's approach to creating the Public Safety Analytics R&D Roadmap include:

- **Lead with Operational Impact:** Rather than trying to capture an exhaustive set of analytics technologies available today and in the future, PSCR chose to begin this process by defining the public safety operational areas that would be most positively impacted through improved data analytics, and then identifying supporting technologies that enable these operational gains. PSCR and the Public Safety Analytics Working Group aimed to limit the scope of this report by discussing how analytics could improve public safety response, communications, prevention, and operations.
- **Devote Sufficient Time and Attention to Defining Technology Gaps:** PSCR hosted a Location-Based Services R&D Summit in October 2015 during which stakeholders improved the technology gaps identified in last year's *LBS R&D Roadmap Report*[1] to develop a set of priority LBS investment areas. Because the Technology Gaps have proven to be instrumental in roadmap follow-up activities, PSCR and the working group dedicated more time and attention to the discussion of analytics technology gaps, barriers, and challenges than they had during LBS.
- **Increase Meeting Cadence:** PSCR decided to increase the frequency of working group meetings during the stakeholder engagement process supporting this report. Whereas the development of the *LBS R&D Roadmap Report* asked stakeholders to participate in bi-weekly conference calls that lasted from 90 to 120 minutes, the Analytics Working Group met weekly for 60 minutes. PSCR decided to apply the logic of the Agile software development cycle[2] to its working group meetings to enable stakeholders to fully immerse themselves and address analytics topics while providing continuous feedback on which gaps and R&D project opportunities should consider in its R&D program execution. This allowed for shorter, more frequent and more focused conversations than the meetings supporting the LBS Roadmap. This helped sustain working group momentum and provided an opportunity for stakeholders to voice their comments, observations, or concerns regarding the direction of the group's discussions.
- **Understand Analytical Workflows:** PSCR built public safety analytics case studies from studying the stages of a typical analytics workflow. When discussing these operational case studies, the working group identified discrete technology capabilities that supported the following stages of Analytics: Data Gathering (Collection, Storage, and Data Organization); Data Processing (Analysis, Modeling, Testing/Evaluation, Interpretation, Machine Learning, and Prediction); and Decision Making (Prediction, Communicating Data and Results, Visualization, Deploying Models & Analytical Rules). By looking at the analytics technology sector through the lens of both Public Safety Operations and Workflow Processes, PSCR sought to make this document relevant to a sufficiently broad audience. A more detailed explanation of the Analytic models that the working group used to scope this report is provided on pages 16-17.

PSCR decided to maintain a consistent R&D roadmap framework so that the trends, capabilities, gaps, and potential project opportunities identified across location-based services and analytics could easily be compared. This consistent framework also lends a common visual logic to these reports.

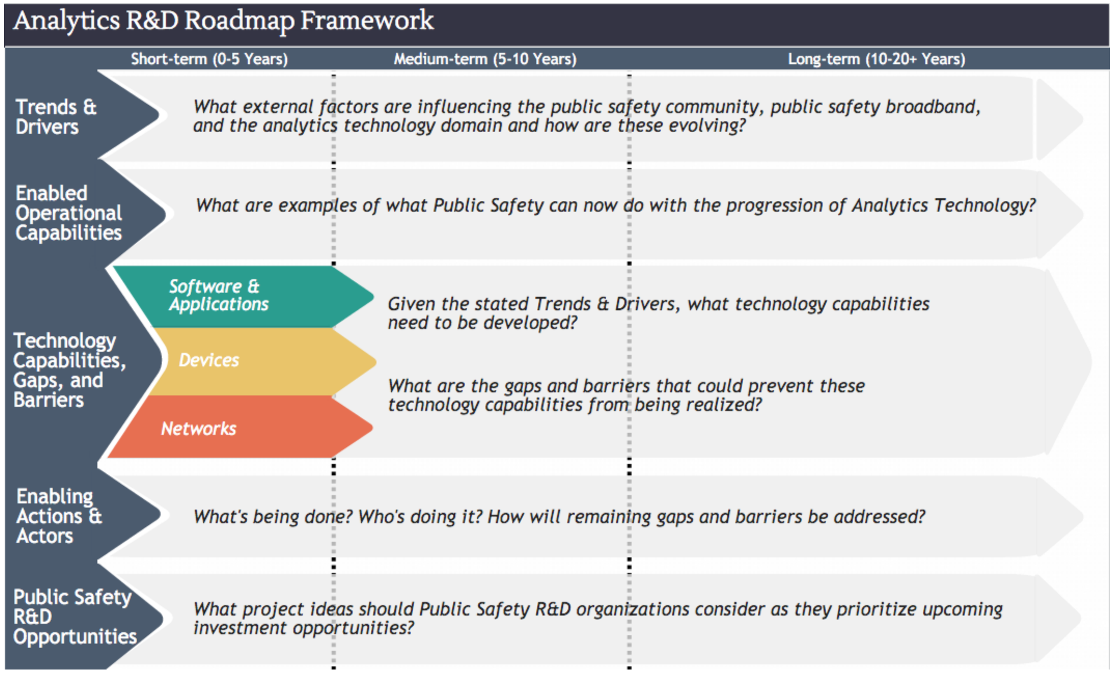
[1] http://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.1883.pdf
[2] http://agilemethodology.org/

Roadmap Framework

Based on the results produced by using the LBS R&D Roadmap framework, a similar framework was customized and created for PSCR's Public Safety Analytics R&D Roadmap (Fig. 2). This framework was used primarily to organize the order of discussions held with the Analytics Working Group. One key component of these roadmap frameworks is the presence of a timeline to give context to the roadmap details and elements. While PSCR is heavily involved in the short-term planning, testing, and evaluation of current technologies, one key outcome of the roadmapping process is to identify technology gaps and opportunities in the medium- to long-term that PSCR can begin evaluating as potential R&D projects. For these purposes, the roadmap was divided into three time frames: short, medium, and long. These time frames were defined in the following manner:

- Short (0 to 5 years) – Straightforward extrapolation of current technology needs
- Medium (5 to 10 years) – Extension of current trends to their reasonable limits
- Long (10 to 20+ years) – Development of major new technologies needed to reach beyond capabilities of current applications

Of course, these timeframes are only projections. Leveraging commercial technologies and targeting R&D investment to critical-path technology gaps can expedite the projected R&D timelines presented in this document significantly.



Analytics R&D Roadmap Framework

Short-term (0-5 Years) | Medium-term (5-10 Years) | Long-term (10-20+ Years)

Trends & Drivers: *What external factors are influencing the public safety community, public safety broadband, and the analytics technology domain and how are these evolving?*

Enabled Operational Capabilities: *What are examples of what Public Safety can now do with the progression of Analytics Technology?*

Technology Capabilities, Gaps, and Barriers: *Software & Applications*, *Devices*, *Networks*

Given the stated Trends & Drivers, what technology capabilities need to be developed?

What are the gaps and barriers that could prevent these technology capabilities from being realized?

Enabling Actions & Actors: *What's being done? Who's doing it? How will remaining gaps and barriers be addressed?*

Public Safety R&D Opportunities: *What project ideas should Public Safety R&D organizations consider as they prioritize upcoming investment opportunities?*

Figure 2: Public Safety Analytics R&D Roadmap Framework

The Public Safety Analytics R&D Roadmap Framework contains four major sections:

- **Trends & Drivers** – PSCR acknowledges that technology is not developed in a vacuum, commercial industry rather than the public safety community often drives advances in analytics technology, and broader events impact the evolution of technology. For these reasons, among others, it was important to begin the roadmapping process by detailing the existing and anticipated trends and drivers within the public safety community, as well as those impacting public safety broadband, and finally, the analytics domain as a whole. The following questions were posed to Analytics Working Group members:
    1. What external factors influence the public safety community and how are these evolving?
    2. What external factors influence public safety broadband and how are these evolving?
    3. What external factors influence the analytics technology domain and how are these evolving?

- **Enabled Operational Capabilities** – A key challenge facing public safety personnel in describing how their operations might differ between now and 20 years in the future is the difficulty in knowing how technology progression may incorporate new and previously unplanned capabilities into operational use. Throughout each technology section of the report (Software & Applications, Networks, and Devices), PSCR has integrated operational examples of how analytics capabilities would support specific public safety operational functions. In addition to these examples, the working group identified four primary Enabled Operational Capabilities that data analytics would provide public safety. These four operational capabilities surfaced as natural themes from the working group's discussion and capture the primary mission areas that would realize greatest benefit from analytics. They include:
    1. Improved Situational Awareness
    2. Improved Decision-Making
    3. Improved Information Management & Data Triage
    4. Improved Network Analytics

    These operational themes helped scope the working group's treatment of analytics technology and ensured that the group primarily focused on capabilities that supported one of the four critical mission areas described above.

- **Technology Capabilities & Gaps –** The majority of the Analytics Working Group's time and attention over the course of 2015 was dedicated to identifying the critical analytics technology capabilities that would go to market and their evolution over time. Once the high-priority technology capabilities were described, the working group identified critical-path technology barriers and gaps that would inhibit these capabilities from becoming adopted by public safety and integrated into their daily operations. Whereas the technology capabilities identified often apply equally to public safety and commercial industries, the gaps and barriers described in this report are unique to analytics deployed in public safety contexts. The technology capabilities and gaps lane was broken down into three categories:
    1. Software & Applications
    2. Devices
    3. Networks

For each sub-lane, the following questions were posed to Analytics Working Group members:

1. Given the stated trends and drivers, what technology capabilities need to be developed?
2. What are the gaps and barriers that will prevent these technology capabilities from being realized?

The data gathered from these questions, Analytics Working Group discussions, and additional market research can be found in sections corresponding to each sub-lane—Software & Applications (page 24), Devices (page 47), and Networks (page 62).

- **Enabling Actions/Actors** – After establishing the technology capabilities and gaps, mapping them to the appropriate sub-lane, and plotting them against the roadmap timeline, Public Safety Analytics Working Group members were asked to identify relevant actors in these fields and specific projects/products that were underway that should inform PSCR's efforts and eventual R&D projects. The following questions were posed to Analytics Working Group members and mapped against each technology capability and gap that had been previously identified:
  1. What's being done?
  2. Who's doing it?
  3. How will remaining gaps and barriers be addressed?

  The data gathered from these questions, Analytics Working Group discussions, and additional market research is discussed briefly in each sub-lane of Technology Capabilities & Gaps (Software & Apps, Devices, and Networks). This concise summary is not intended to be comprehensive of the full spectrum of analytics-related R&D occurring in today's technology marketplace. Rather, these enabling actions and actors represent leverage points for public safety to take advantage of market-ready technologies and make them public safety grade.

- **Public Safety R&D Opportunities** - Given the technology capabilities, gaps and barriers, and enabling action and actors that are forecasted to impact the analytics domain over the next 20 years, the Analytics Working Group identified potential R&D efforts Public Safety R&D organizations should consider as they prioritize upcoming investment opportunities. These R&D opportunities will be the expanded upon by a larger stakeholder group at the upcoming PSCR Public Safety Analytics R&D Summit, scheduled to take place in the late summer 2016.

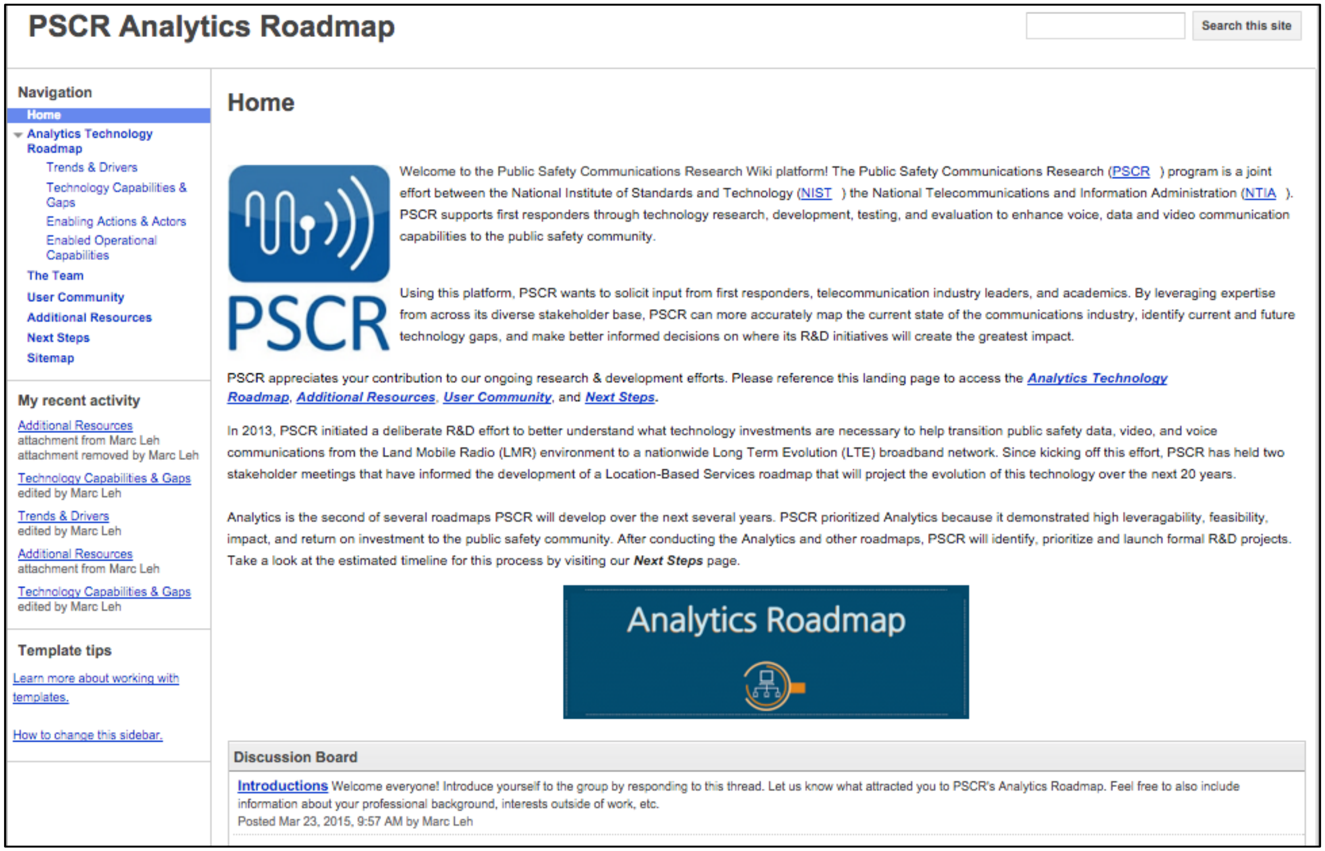
Stakeholder Involvement Strategy

PSCR's Public Safety Analytics Working Group consisted of over 60 stakeholders from public safety, industry, academia, and all levels of government. To recruit these stakeholders, PSCR sent out a formal invitation to its list of Cooperative Research and Development Agreement partners, contacted early adopters of data analytics in public safety, and engaged representatives with leading big data technology providers. PSCR officially kicked off the Public Safety Analytics Working Group in May 2015 and held meetings until December 2015. One-on-one interviews were also conducted with the following individuals/agencies, as they had been identified as leading users of public safety analytics-related technology by PSCR support staff:

- Deputy Chief Eddie Reyes – Alexandria, VA Police Department
- Jason Schiess – Durham, N.C. Police Department
- Elizabeth Gray – Austin, TX Fire Department

Special thanks Deputy Chief Eddie Reyes and the Alexandria Police Department for hosting the PSCR Support staff to observe the use of analytics in daily operations briefings.

Similar to the approach used to collect input for the LBS Roadmap, the PSCR support team created a collaborative Wiki platform (Fig. 3) that participants could use to capture their expertise, provide recommendations, and review outcomes from past meetings. The PSCR Analytics Wiki Platform can be accessed at https://sites.google.com/a/corneralliance.com/pscr-analytics-roadmap/.


Search this site
Navigation
Home
Analytics Technology Roadmap
Trends & Drivers
Technology Capabilities & Gaps
Enabling Actions & Actors
Enabled Operational Capabilities
The Team
User Community
Additional Resources
Next Steps
Sitemap
My recent activity
Template tips
Learn more about working with templates.
How to change this sidebar.
PSCR
Analytics Roadmap

PSCR Analytics Roadmap

Home

Additional Resources
attachment from Marc Leh
attachment removed by Marc Leh

Technology Capabilities & Gaps
edited by Marc Leh

Trends & Drivers
edited by Marc Leh

Additional Resources
attachment from Marc Leh

Technology Capabilities & Gaps
edited by Marc Leh

Welcome to the Public Safety Communications Research Wiki platform! The Public Safety Communications Research (PSCR) program is a joint effort between the National Institute of Standards and Technology (NIST) the National Telecommunications and Information Administration (NTIA). PSCR supports first responders through technology research, development, testing, and evaluation to enhance voice, data and video communication capabilities to the public safety community.

Using this platform, PSCR wants to solicit input from first responders, telecommunication industry leaders, and academics. By leveraging expertise from across its diverse stakeholder base, PSCR can more accurately map the current state of the communications industry, identify current and future technology gaps, and make better informed decisions on where its R&D initiatives will create the greatest impact.

PSCR appreciates your contribution to our ongoing research & development efforts. Please reference this landing page to access the ***Analytics Technology Roadmap***, ***Additional Resources***, ***User Community***, and ***Next Steps***.

In 2013, PSCR initiated a deliberate R&D effort to better understand what technology investments are necessary to help transition public safety data, video, and voice communications from the Land Mobile Radio (LMR) environment to a nationwide Long Term Evolution (LTE) broadband network. Since kicking off this effort, PSCR has held two stakeholder meetings that have informed the development of a Location-Based Services roadmap that will project the evolution of this technology over the next 20 years.

Analytics is the second of several roadmaps PSCR will develop over the next several years. PSCR prioritized Analytics because it demonstrated high leveragability, feasibility, impact, and return on investment to the public safety community. After conducting the Analytics and other roadmaps, PSCR will identify, prioritize and launch formal R&D projects. Take a look at the estimated timeline for this process by visiting our ***Next Steps*** page.

Discussion Board

Introductions Welcome everyone! Introduce yourself to the group by responding to this thread. Let us know what attracted you to PSCR's Analytics Roadmap. Feel free to also include information about your professional background, interests outside of work, etc.
Posted Mar 23, 2015, 9:57 AM by Marc Leh

Figure 3: Analytics Wiki created to capture working group input

Introduction to PSCR Public Safety Analytics R&D Roadmap

Just as PSCR researched and developed its own definition of LBS to frame the subject in proper context, the Analytics working group validated the following definition of analytics to scope the subject for public safety. ***Analytics, as defined in this roadmap, refers to the scientific process of transforming data into insight for making better decisions[3].*** This definition was intentionally broad to allow the Analytics Working Group to evaluate the full range of Software, Network, and Device technologies that could potentially deliver value to public safety response, communications, and operations. The operational objectives outlined in this report brought necessary scope to this definition when the working group began to identify discrete technology capabilities that could enhance public safety job efficacy. As a result, this roadmap focuses on how the technology and scientific techniques that collect, process, and analyze source data can transform information into valuable intelligence for public safety.

To help scope the data collection process, the Analytics Working Group developed a high-level overview of a typical analytics workflow (Fig. 4) to better understand the mechanics of how organizations mine, transform, and filter data to improve business processes. The group was asked to keep the various stages of the analytics workflow in mind when evaluating the relevance and feasibility of various analytical tools in public safety agencies.. Many of the technology capabilities, gaps, and recommended R&D project areas relate to one or several of the following stages of analytics:

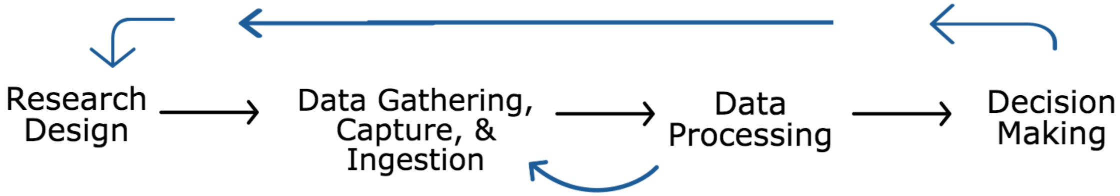


Figure 4: Analytics Workflow Overview developed by Analytics Working Group

1. **Research Design –** The first step in designing analytics solutions that provide value to an organization is to identify and define a specific problem or challenge that an organization would like to solve. By thoughtfully defining the problem, objective, and overall research design of your analytics solution from the outset, data scientists are better equipped to identify relevant data sources that would deliver valuable insight into this challenge and design analytic systems that manipulate these sources in meaningful ways for the end-user.
2. **Data Gathering, Capture, and Ingestion –** The next stage of the analytics workflow is to successfully acquire the information to be analyzed. Technology will need to collect, store, organize, and transform data into a standardized format before processing, and there are a variety of tools to

[3] https://www.informs.org/About-INFORMS/What-is-Analytics

support these functions that are described later in the report. Techniques used for preparing data for processing include integrating or aggregating data feeds, transforming datasets into a common format, removing unnecessary or harmful data points, or filtering records by feature.

3. **Data Processing –** After collecting and preparing source data, information must be processed to uncover relationships, trends, and overall intelligence hidden within the input data. Common data processing techniques use a combination of statistical modeling, model testing and evaluation, and machine learning to build automated systems that can organize and learn from source data.
4. **Decision Making –** After processing raw or prepared data through an analytic system, organizations must still draw conclusions from the process information and begin to make better decisions. To better inform or justify their decisions, organizations may use processing results to predict what is likely to happen in the future, communicate their results through data visualization, or deploy additional models or rules to improve the accuracy or relevance of their data processing.

Despite the seemingly linear workflow outlined above, data analytics is an extremely iterative discipline. Figure 5 below illustrates how effective data scientists must alternate between executing analytical processes, reflecting on the results, and disseminating satisfactory conclusions externally or to other internal applications. The working group agreed that organizations seeking to draw meaningful intelligence out of raw data need to continuously interact with and refine their analytics methodology. This could mean seeking new information sources to acquire, filtering source data by different features, or redesigning processing models altogether after interpreting initial findings. By continuously reflecting on analytic experiments and exploring potential alternatives, researchers will be in a stronger position to understand analytic outputs, scale technologies across their organization, and share results with like-minded peers.

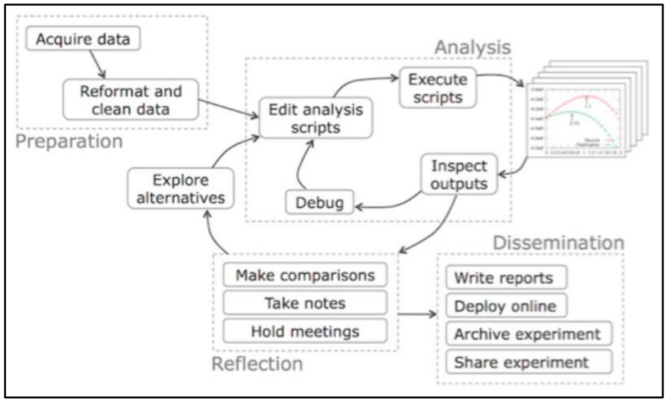


Figure 5: Diagram illustrating relationships between the stages of an Analytics workflow[4]

[4] http://m.cacm.acm.org/blogs/blog-cacm/169199-data-science-workflow-overview-and-challenges/fulltext

Considerations for Public Safety's Expanded Use of Analytics

The Analytics working group consistently expressed that the decision to deploy new data analytics technology in public safety agencies needs to take into consideration several environmental realities given the sensitivity and complexity of public safety's mission. While some of the considerations below were initially identified in the *LBS R&D Roadmap*, the concepts remain applicable to the Public Safety Analytics R&D Roadmap. Although not the focus of this report, the following considerations should be evaluated before prioritizing or launching a formal analytics R&D project:

- **Privacy –** Monitoring proprietary or individual citizen data may raise privacy concerns. Public safety must anticipate these concerns and develop clear expectations that define why public safety needs and is authorized to use sensitive data sources.
- **Regulatory –** Legal, statutory, and regulatory considerations may make it difficult or impossible for public safety to access data sources that would otherwise be valuable inputs into analytical systems. Public safety agencies need to fully understand the legal implications of their data analysis prior to designing, procuring, or implementing analytical systems.
- **Staffing –** Changes/advances in technology may require additional staffing (hours or personnel) to take on analytics implementation and support once up and operational.
- **Policy –** For public safety's best interests, standard operating procedures and policies will need to be created before analytics technologies can be properly used.
- **Training –** Adequate initial training and refresher training is needed to ensure users are familiar with new analytics technologies.
- **Funding –** Long-term planning is needed to adequately fund the local adoption and implementation of emerging analytics technologies. This is relevant for equipment purchases, computing resources, as well as increased staffing needs.
- **Clear Benefit –** While some analytics solutions may facilitate operational efficiencies, others may add responsibilities or undue burden onto already busy public safety individuals and organizations. A clear benefit to public safety operations must be evident that outweighs the potential added responsibilities or burden to the public safety community.
- **Legal Authority –** Sharing resources between public and private sectors or between different levels of government requires significant legal research on all levels of government to ensure that legislation is being followed and that it is not being violated. Legal agreements may need to be further researched or executed before launching collaborative analytics R&D projects or implementation initiatives.

Trends & Drivers

What external factors are influencing the public safety community, public safety broadband, and the Analytics technology domain and how are these evolving?

Key to PSCR's roadmapping efforts is the contextual understanding of how technology capabilities evolve – not only in terms of the technology itself, but also the larger environment in which the technology evolution is taking place. The Analytics Working Group members identified trends and drivers across three specific focus areas:

1. Trends and drivers impacting public safety
2. Trends and drivers impacting public safety broadband
3. Trends and drivers impacting the analytics domain

As stated in PSCR's Public Safety Broadband Research and Development Roadmap – Beginning the Process report, key trends and drivers impacting all of these areas include:

- Shrinking budgets at the federal, state, and local levels;
- A move toward regionalization of response;
- The impact of the secondary responder community in a more broadly defined public safety response role, and;
- The changing role of the public in emergency response through social media, mobile apps, and citizen reporting.

While not a primary focus of this report, security and privacy concerns were discussed given the potential impact they have on the application and use of analytics in public safety planning and response. In particular, while technology capabilities do and in the future will more holistically enable the analytics of data from numerous sources, security and privacy issues must be addressed to ensure the appropriate use of these evolving capabilities.

Trends & Drivers

Public Safety

Short Term – 0 to 5 years (A straightforward extrapolation of current technology needs)

- **Demand**
  There is an increasing demand for ubiquitous data connection for the public safety community. Due to the consumerization of IT, public safety is demanding more and better software application features and mobile support. There is also a public demand for more transparency through the use of open data technologies and policies.

- **Use**
  While the Internet of Things (IoT) is creating vast data streams, public safety is struggling to determine how to gain access to the data, and once afforded access, what to do with all of the information. There is also immediate public scrutiny regarding how the data is being used by public safety. Big data analytics will continue to revolutionize how public safety manages networks and prioritizes services in real time.
- **Community Relations**
  Police procedures in identifying and apprehending suspects are under increased scrutiny.

Medium Term – 5 to 10 years (Extension of current trends to their reasonable limits)

- **Wider availability of broadband data leading to an exponential increase in the need to manage data**
  Analytics will play a key role in data management. Advancements could see a reduction in bandwidth needs for specific applications that are able to offload analytic processing to the edge as opposed to transmitting large amounts of data back to the network core to be processed.
- **Opportunities for public safety to harvest and leverage public and private data comes into focus**
  Policy, legal, and technological advancements will enable public safety access to large amounts of data previously unavailable to the community. Access to these large data sets could lead to significant improvements in public safety's ability to plan for, respond to, and recover from incidents.

Short, Medium, and Long Term – 0 to 20+ years

- **Coordination**
  In response to the increased need for better coordination and information sharing between public safety entities, there will be an increasing trend of gathering, analyzing, and sharing information with those who need it.
- **Current Events**
  Current events such as natural disasters, disease outbreaks, and terrorist attacks will drive the focus and funding opportunities for technology advancements both within the public safety community and the larger environment.

Trends & Drivers

Public Safety Broadband

Short Term – 0 to 5 years (A straightforward extrapolation of current technology needs)

- **Increased Scrutiny from Videos**
  Ubiquitous nature of body worn, dash cameras, and video from the general public being used as a constant critique of public safety services.
- **Potential Paradigm shift from LTE-U Capabilities**
  The shift for public safety from dedicated-only spectrum to unlicensed spectrum that will improve coverage of public safety networks, add improved data rates in common operating scenarios, and serve as backhaul offloading mechanism that will decrease operating costs for public safety cellular carriers.

Medium Term – 5 to 10 years (Extension of current trends to their reasonable limits)

- **Movement towards standardization**
  There is a need to standardize the ways to produce data so that it is consumable for public safety agencies, both within and across jurisdictional boundaries. Interoperability for analytics will better enable chaining together analytical outputs from different organizations.
- **Need to define 'mission-critical' data in context of prevalent 'Big Data'**
  Public safety will continue to refine its definition of mission-critical data in relation to the pervasiveness of big data available to agencies. Wearables will be one generator of big data, though it is yet to be determined what analytics on wearables will look like or enable.
- **Emergence of 5G and M2M**
  Next-generation technologies like 5G and Machine-to-Machine (M2M) communications will usher in new capabilities and challenges to public safety agencies looking to capitalize on these technological advancements.
- **Analytics on deployables**
  Public safety will need to determine what analytics will be needed and used on deployables and the associated requirements.

Short, Medium, and Long Term – 0 to 20+ years

- **IP as inefficient means of sending data**
  Network function virtualization and software-defined networks will continue to evolve and include instances of micro evolved packet cores.
- **Gathering and sharing of information is often conducted via wireless (broadband) links. IoT enabling much larger source of data for consumption and distillation**
  Needing to collect, analyze, and deliver vast datasets to the "right place at the right time" could overwhelm network during significant events.
- **Increasing potential for cyber attacks, possibly in coordination with physical attacks. This will drive an increased demand for real-time sophisticated situational awareness**
  Response to such events will require coordinated analytics of both the cyber and physical worlds to best direct public safety operations.
- **Trends towards small cells, densification, and general Heterogeneous Network (HetNet) asset integration into overall public safety network will enable greater coverage, improved bandwidth ability, and lead to gains in redundancy and reliability**
  Self-organizing networks are key to HetNet integration. Integration and management will be automated because of the magnitude of assets composing the network.
- **Demands for data transparency and privacy significantly increase**
  Public demands for increased transparency into public safety operations and decision making will be met with an increased need to protect privacy in relation to data access.

Short Term – 0 to 5 years (A straightforward extrapolation of current technology needs)

- **Cultural and Organizational changes spurred by application of analytics in public safety**
  As analytics capabilities advance, public safety will need to develop a level of trust in the outcomes of analytical results to fully integrate the capability into their daily operations. There is a potential challenge of "if you build it, they will not come", if users and leaders do not understand the benefits of analytics. There also may be needed organizational or operational changes needed to fully realize the capabilities of analytics.
- **Advances in Internet of Things, Social Media Analytics, and Cognitive Analytics**
  The use of analytics in other sectors such as healthcare will drive improvements in wearables and relevant analytical capabilities for the public safety community. The ability to 'personalize' results produced from analytics will further enable a deep integration into public safety operations.
- **Need for both voice and high-speed data from first responders**
  Operational needs from public safety will drive analytics platforms evolving to understand the performance of both the application layer and underlying communication infrastructure.

Short & Medium Term – 0 to 10 years (Extension of current trends to their reasonable limits)

- **Increasing sophistication of machine learning and computing technologies**
  The R&D community will invest significant resources in developing machine learning technology for text, video, and audio. Specifically, social media analytics will be one of the driving industry segments. The mobile device market will drive advances in speech recognition. Textual analytics will likely become much more sophisticated. Federal investment in data resources, including ground truth, remains a critical driver outside of commercial industry.
- **Public safety defining storage capabilities and policies**
  Public safety will need to determine how to intelligently store data and develop related retention policies. Storage policies may initially differ from discipline to discipline and be subject to applicable state or jurisdictional laws. Public safety must also consider the storage of raw data vs. processed data and analytical results. Finally, public safety must be able to perform analytics on stored data as well as conduct search, playback, and redaction functions.

Long Term – 10 to 20+ years (Development of major new technologies needed to reach beyond the capabilities of current approaches)

- **Cost of technology becomes largely commoditized**
  As advancements in analytics continue over the next several decades, the technology itself will become largely commoditized. The value of the data will be in the application of its results. Public safety could stand to benefit from this commoditization, but also must continue to clearly define requirements and desired outputs it wants from the data.

- **Accelerated technology refresh cycle presents unique challenges to public safety**
  Continual costs of technology upgrades and replacements for public safety presents the challenge of integrating differing technologies and data sets into a common and shared ecosystem. Public safety will be presented with the challenge of integrating sources and content to present a consistent data set across a wide variety of users.

Short, Medium, and Long Term – 0 to 20+ years

- **Evolution of analytical capabilities driving use for public safety**
  Public safety will benefit from advancements in areas such as visualization and video analytics techniques across multiple geographically diverse server/cloud/data warehousing systems as well as the growth of facial recognition and object recognition/image identification. Facial Recognition software eventually integrates with public data sources.
- **Ability of analytics to prevent and/or mitigate impact of cyber attacks**
  Public safety is able to re-route data over a backup path if the primary path is attacked or down due to technology failure or cyber attack. Analytics will also drive the predictive modeling of attack vectors.
- **Anticipation of massive amounts of raw data ingested, consumed, and information extracted**
  Public safety's access to and processing of big data has implications for storage and computational resources required to analyze the data for meaningful insight. There is the potential for massive amounts of data for ingestion and decision-assisting purposes with the added complication of potentially actuating an automated corrective action for public safety purposes. The rising trend in smart cities, smart buildings, smart utilities, and in general that of smart infrastructure will drive the growth of the big data from which public safety will need to derive meaning and value.
- **Analyzing both structured and unstructured data**
  Public safety will be able to take advantage of different types of unstructured data by combining it with structured data that can then be analyzed. Elastic search capabilities could be a driver for enabling the analytics of unstructured data.

Technology Capabilities, Gaps, and Barriers
Software & Applications
Devices
Networks
Given the stated Trends & Drivers, what technology capabilities need to be developed?
What are the gaps and barriers that could prevent these technology capabilities from being realized?

Software and Applications

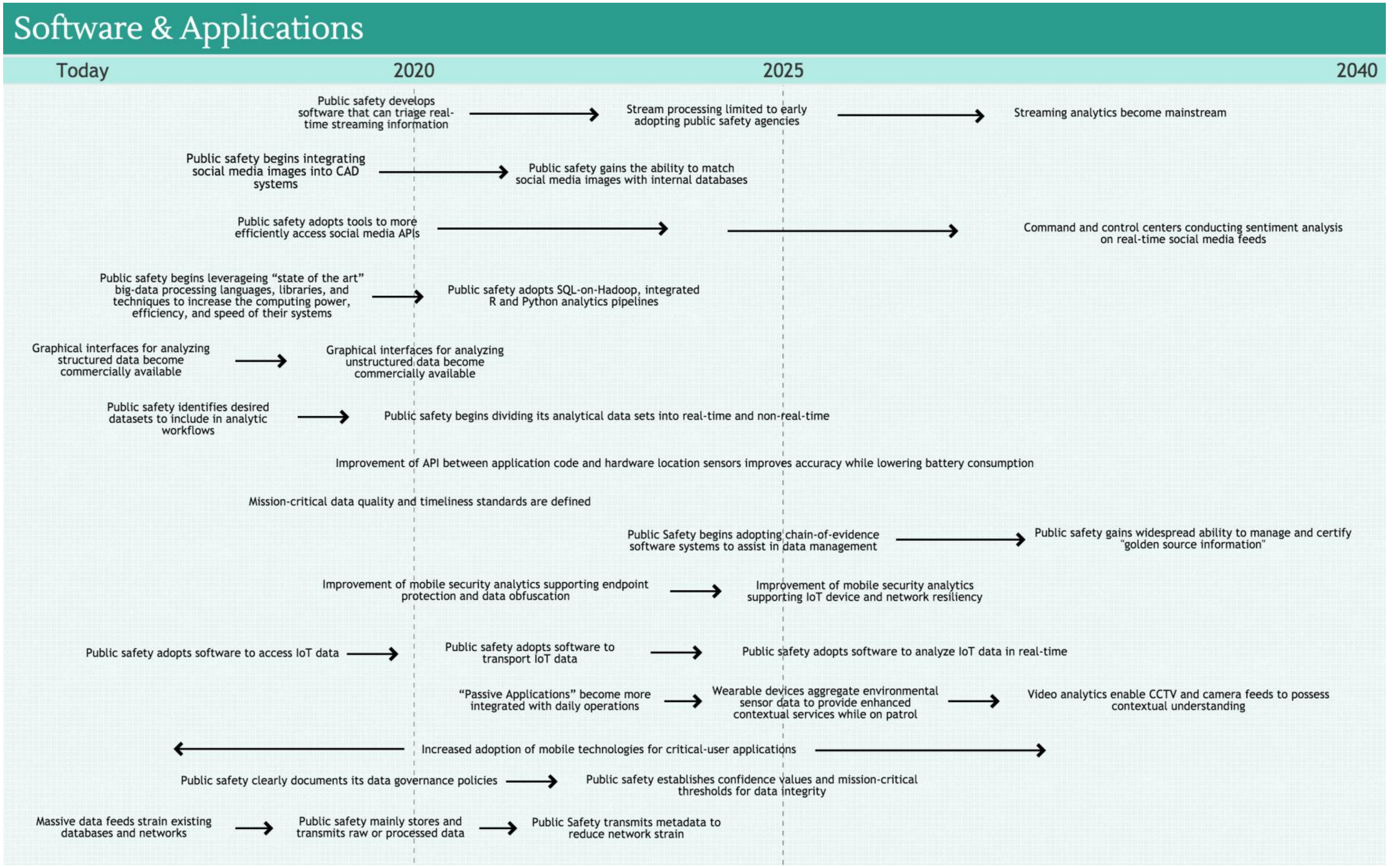
The processing power and sophistication of modern analytical systems has increased in recent years. With companies and government organizations seeking greater insight into their stakeholders' motivations, demographics, and behavioral patterns, applications that can both synthesize disparate data sources and facilitate improved data processing have become incredibly valuable in the age of big data. Commercial industry has invested significant resources into developing off-the-shelf applications that mine datasets, predict patterns, build statistical regression or classification models for customers themselves to generate intelligent, usable information from raw – and even unstructured – data.

While public safety ideally will be able to leverage the intellectual capital, products, and services available in the analytics technology marketplace today, the sensitivity of information that public safety agencies seek to analyze, local control issues, and security concerns will present unique challenges to integrating current platforms into public safety information systems.

Given the immense scope, complexity and end-use of the analytics software technology domain, PSCR asked the Analytics Working Group to forecast the evolution of the most important underlying technology capabilities in light of the trends & drivers discussed earlier.

After taking inventory of the variety of technical abilities, gaps, and challenges facing public safety's increased use of analytical software over the next 5, 10, and 20+ years several themes became clear. Nearly all of the technology capabilities and gaps the working group identified in the Software & Applications lane related to one of the following two operational objectives:

1. Integration of Multiple Data Sources
2. Improvement in Data Processing Capabilities



Software & Applications

Today | 2020 | 2025 | 2040

Public safety develops software that can triage real-time streaming information → Stream processing limited to early adopting public safety agencies → Streaming analytics become mainstream

Public safety begins integrating social media images into CAD systems → Public safety gains the ability to match social media images with internal databases

Public safety adopts tools to more efficiently access social media APIs → → Command and control centers conducting sentiment analysis on real-time social media feeds

Public safety begins leverageing "state of the art" big-data processing languages, libraries, and techniques to increase the computing power, efficiency, and speed of their systems → Public safety adopts SQL-on-Hadoop, integrated R and Python analytics pipelines

Graphical interfaces for analyzing structured data become commercially available → Graphical interfaces for analyzing unstructured data become commercially available

Public safety identifies desired datasets to include in analytic workflows → Public safety begins dividing its analytical data sets into real-time and non-real-time

Improvement of API between application code and hardware location sensors improves accuracy while lowering battery consumption

Mission-critical data quality and timeliness standards are defined

Public Safety begins adopting chain-of-evidence software systems to assist in data management → Public safety gains widespread ability to manage and certify "golden source information"

Improvement of mobile security analytics supporting endpoint protection and data obfuscation → Improvement of mobile security analytics supporting IoT device and network resiliency

Public safety adopts software to access IoT data → Public safety adopts software to transport IoT data → Public safety adopts software to analyze IoT data in real-time

"Passive Applications" become more integrated with daily operations → Wearable devices aggregate environmental sensor data to provide enhanced contextual services while on patrol → Video analytics enable CCTV and camera feeds to possess contextual understanding

← Increased adoption of mobile technologies for critical-user applications →

Public safety clearly documents its data governance policies → Public safety establishes confidence values and mission-critical thresholds for data integrity

Massive data feeds strain existing databases and networks → Public safety mainly stores and transmits raw or processed data → Public Safety transmits metadata to reduce network strain

Operational Objective: Analytics Enabling More Seamless Integration of Multiple Data Sources

Data Integration, or the "combination of technical processes to combine data from disparate sources into meaningful insight and information[5]," ideally yields a complete, unified range of information to consider inputting into an analytical process. By 2020, some researchers estimate that 15-40 billion additional connected devices will hit the market[6]. As the volume of data available to data scientists, programmers, and organizational leaders continues to increase, it is necessary to effectively fetch accurate, meaningful data – regardless of where it resides – and manipulate this data to gain enhanced business or operational intelligence. Within the context of public safety, integrating multiple data sources is important because it allows inter-jurisdictional agencies to merge data sources to provide a more comprehensive overview of a region, situation, or trend to be analyzed.

While this section will emphasize the need for public safety to seek a better understanding of the data sources available to the community, it hopes to identify the underlying capabilities that would enable public safety agencies to synthesize disparate data sets – whether stored in cloud databases, environmental sensors, IoT endpoints, or government data centers – into a single analytical workflow.

Enabled Operational Capabilities

The Analytics Working Group identified three primary operational capabilities that would benefit from R&D focusing on enhancing public safety's ability to integrate multiple data sources through software & applications. These include:

- Improved Situational Awareness
- Improved Decision Making
- Improved Information Management & Data Triage

Technology Capabilities, Gaps, and Barriers

The Analytics Working Group identified several key gaps and barriers associated each technology capability that need to be addressed before the ability to integrate multiple data sources via software and applications becomes a reality for public safety. Some of the most commonly identified gaps inhibiting public safety's ability to integrate multiple data sources included the lack of common data standards and public safety's inability to ingest and process unstructured data. The working group also cited that even structured datasets available to public safety today have varying levels of quality and formatting; and that reconciling existing database structures with new data created by emerging technologies such as IoT and video streaming would pose additional challenges in the short- to medium-term. One of the most fundamental barriers to seamless data integration is simply a lack of awareness or access to datasets that are accurate, current, and relevant to improving response. If public safety could browse a centralized data repository that stored or referenced trusted information, the community could more confidently define its purpose for collecting data, who is responsible for collecting and verifying it, and how these analytic tools support specific public safety activities.

[5] http://www.ibm.com/analytics/us/en/technology/data-integration/

[6] http://www.datanami.com/2015/09/22/the-data-of-things-how-edge-analytics-and-iot-go-hand-in-hand/

1. Analytics Software improves IoT integration across first responder-worn body devices and environmental sensors.
In response to the rapid proliferation of data created by network-equipped IoT devices being deployed in our homes, offices, and cities today, the working group anticipates that the software that acquires, transports, and analyzes this IoT data will mature greatly over the next 0-5 years. Public safety will need to leverage the data created and captured by IoT devices and environmental sensors such as body cameras, microphones, biological vital sensors, building controls, public transportation, smart grid power, and other fixed municipal infrastructure. To garner intelligence from this, public safety will likely first seek to improve the integration of responder-worn devices and environment/utility devices so that there is seamless information exchange between the responder and his or her environment when on patrol.

Gaps & Barriers
Lack of common standards and processing models for specific public safety support activities.
Ability to process and distill source data into meaningful outputs and predictors for operational personnel.
Need a more secure, reliable means of integrating IoT data.
Need better ability to integrate and analyze video data collected from sensors on public safety networks and devices.
Need to determine whether public safety will conduct analytics "on the edge" (on the IoT device) or in a more centralized processing location.
Lack of body-worn, vehicle-based, Bluetooth, and/or Wi-Fi-enabled data integration software.
Data integration software must seamlessly transmit aggregated datasets across Wi-Fi, Bluetooth, 4G, and 5G LTE broadband networks.
Public safety does not possess software that can aggregate, filter, transform, and process unstructured data created by IoT devices today.
Current Public Safety software systems do not have sufficient bandwidth to download and upload massive IoT and sensor data streams.

2. **Software allows analysis across a number of applications and databases, leading to the ability to simultaneously search multiple datasources in real-time for a specific piece of information.**

In addition to facilitating improved information exchange between responder-worn IoT devices and relevant environmental sensors, public safety will need to seek to combine this data with information stored across a number of existing applications and databases at their disposal. A potential capability would be an application that automatically mines information from drivers license and social media accounts based on the license plates observed by an on-vehicle video camera while on patrol. Other situational awareness benefits resulting from analytics' ability to scan multiple, disparate databases for specific intelligence could take the form of a live video feed that can recognize characters or contextually understand what is happening in an environment due to the behavior of people, objects, or vehicles in the vicinity.

Gaps & Barriers
Disparate levels of data quality and type in each database.
Need to align metadata standards across jurisdictions so that organizations can conduct an efficient analysis when data sharing agreements are in place.
Lack of open source data science expertise in public safety settings.
Limited use of open source data integration platforms in public safety settings because of regulatory challenges or data sharing agreements.
Public Safety lacks the ability to discern "golden source" information – or deciphering multiple, overlapping records for the 'true' data point.
Limited access to non-public safety camera feeds and other data centers.
Weak or nonexistent public safety data standards.
Inability to match images (from security cameras, CCTV, DMV records) with audio, video, structured text, unstructured text, and database records.
Live video feeds do not feature automated character, object, or behavior recognition.

3. Increased adoption of mobile technologies for critical-user applications.

The Analytics Working Group also projects that public safety will increase its adoption of mobile technologies for mission-critical user applications, and that analytic software will become increasingly embedded in public safety devices or become more device-dependent. For example, responders will achieve greater situational awareness if they possess ruggedized wearable devices that can aggregate environmental sensor data to provide enhanced contextual services while on patrol. To power this capability, public safety devices will need to run local applications that can simultaneously search, transform, and aggregate specific pieces of information to use as inputs into the models, algorithms, or software systems that process this data to present actionable recommendations.

Gaps & Barriers
Need for more sophisticated security software related to Mobile Device Management (MDM), Mobile Application Management (MAM), and Mobile Content Management (MCM).
Need to compile a prioritized list of critical on-device applications desired by first responders.
Need to collect and document mobile software requirements from public safety lead users & early adopters of mission-critical mobile applications.
Devices will need much greater power and memory capacity to run analytic software locally.
Need to define "tripwire" requirements that cause device-embedded analytic software to trigger an action/alert based on data aggregated and processed on the device.

4. Increased sophistication of public safety data governance allows for more accurate and efficient integration of disparate data stores.
As Public Safety endeavors to find software systems that accurately and effectively merge disparate data sources into a single, trusted source of truth, sound data governance procedures will become increasingly important in its development and adoption of business intelligence products. Establishing clear Data Governance programs, or the "overall management of the availability, usability, integrity, and security of the data employed in an enterprise[7]," will help public safety agencies clearly define what data is of value to their mission, why it collects this data, who is responsible for collecting and securing it, and how it plans to transform this data into intelligence that will improve public safety processes. Some working group participants believed that by answering these questions, public safety would be better equipped to document their implemented or desired analytical workflows which would lead to more effective and defensible software systems that support improved decision making. Enhanced data governance would also help public safety understand the data sources available to their agency and ensure that their analytical systems ingest the most accurate or relevant data available to them.

The Analytics Working Group recommended that public safety should pursue Golden Source recordkeeping – or a single version of all data in an organization that is verified to be true[8] – for the data that it controls, and seek to establish confidence values for 3rd party data providers or data that public safety merges with data from external organizations.

Gaps & Barriers
Public safety agencies must more clearly define its desired outcome(s) for integrating and analyzing disparate data sources.
Need to define data standards related to semantic content, data handling, and protection.
Need to define standards for sharing source data and extracted metadata.
Lack of a national compendium of data sources available to or specifically designed for public safety purposes.
Must improve the security provided by authorization and authentication of data set users.
Public safety needs a better understanding of the data available and unavailable to them.
Need for a strong "Golden Source" certification process that will deliver increased confidence in the accuracy of data ingested into public safety analytics software.
Challenge of applying multi-dimensional data to existing databases while maintaining data integrity.
Lack of standards or interfaces that enable agencies to exchange data with disparate versioning and formats.
Software's reliance on databases not controlled by public safety.
Implementing quality assurance practices to establish golden source verification processes demand significant time and cost.

[7] http://searchdatamanagement.techtarget.com/definition/data-governance
[8] http://whatis.techtarget.com/definition/golden-record

5. Public safety collects more data more efficiently through increased use of passive applications and analytics at the edge.
Another technology capability that was highlighted by the working group as improving Public Safety's ability to merge multiple data sources is the rise of "passive applications" becoming more integrated with daily operations. This capability could take shape as a latent video camera that runs during vehicle patrol scanning for suspicious activity (i.e. speeding or erratic drivers) and identifying characteristics (i.e. facial recognition or license plate number), and cross references with external data points such as statewide arrest records or alerts. While iterations of this technology are available today in the form of dashboard cameras or on-body video cameras, current public safety analytics software systems cannot capture and transmit the massive video data streams to other databases. The eventual convergence of Enterprise, Social, Mobile, and Cloud technologies underscores the importance of public safety developing or adopting systems that can seamlessly collect, filter through, and aggregate data stored in these repositories for its own processing and decision making.

Finally, the working group projects that public safety will transition from collecting and storing raw data in bulk to transferring more metadata and performing analytics at the edge in the next 5-10 years. Public safety will be enabled to do this through increased use of modern, lightweight Application Program Interfaces (APIs) and through sensors equipped with their own analytic systems. By installing more analytic applications that generate intelligence at the point of data creation or collection, public safety will reduce network traffic and increase processing speed by alleviating bandwidth constraints or network congestion that occurs when forced to transmit large data streams such as video from the field to a central processing facility.

Gaps & Barriers
"Passive" applications currently do not include a command/control function to trigger the active state and deliver high-priority data to the responder.
Lack of sophisticated sensors or analytic tripwires to trigger applications from passive to active state.
Lack of standard parameters for multi-variable control software to ensure that software is directing response in the same way as other responding agencies.
General inability to process unstructured data such as video, audio, and free form text.
Analytic systems do not account for video data characteristics such as increased size and memory requirements.
Lack of widely available processing power for simultaneous triage of data from social, mobile, analytics, and cloud technologies.

6. **Data visualization and integration software presents a more consistent, reliable view of combined and federated data to public safety operational command and on-scene command.**

Centralized data collection and processing centers, such as a Public Safety Answering Point (PSAP) aggregating and analyzing disparate data sources, will eventually be able to send model results to responders on scene. For example, the PSAP may eventually maintain a data integration system that processes building system information such as fire alarm pull station locations, smoke detector activation locations, and ventilation systems while looking for patterns and status changes that indicate incident severity.

Gaps & Barriers
PSAPs do not automate technologies to integrate information from disparate data sources.
PSAPs and other centralized information processing centers need software that will ingest, match, and provide initial severity analysis of input data.
Interoperability concerns with public safety data integration systems.
Significant need for public safety data intake standards.
Public safety's reliance on proprietary rather than open-source software.
Software systems need the ability to validate the authenticity of data that is "pushed-to" or "pulled-by" centralized public safety database.
Current content analytics and speech recognition algorithms are immature and not integrated with dispatch or public safety data centers.

Enabling Actions & Actors

What's being done? Who's doing it? How will remaining gaps and barriers be addressed?

This section is not intended to serve as an exhaustive review of all actions and actors supporting public safety's ability to integrate multiple data sources into analytical processes. Given the breadth of commercial, academic, and government activities relating to Open Data, analytical software development, and data management, continued market research will be necessary to ensure awareness for PSCR of current efforts and account for new actors in the analytics domain.

Open Source Data Integration

- University of Southern California, Information Sciences Institute – The University of Southern California's Information Sciences Institute has published Karma, an application that integrates data from sources such as databases, spreadsheets, text files, ML, JSON, and Web APIs, with support from the Defense Advanced Research Projects Agency (DARPA), the Air Force Research Laboratory, the National Science Foundation (NSF), and the National Institutes of Health (NIH)[9]. Karma uses a graphical interface to map disparate data points to ontology classes, or defined names, properties, and interrelationships of the original datasets ingested. In a recent case study[10], Karma integrated publicly available oil well and road network geolocation data from a United States Geospatial Service (USGS) map to help first responders optimize evacuation plans in the event of an oil field fire.
- Talend – Talend's data integration platform uses over 900 prebuilt components to synchronize locally stored and cloud-based datasets in a centralized repository. It's source code and core modules have been published open-source under the Apache license. In addition to synchronizing and cleaning data so that disparate data stores can be analyzed in a standardized format, Talend's platform allows users to extract and manage metadata[11].
- Pentaho – Pentaho's open-source business intelligence suite enables its community of over 13,000 users[12] to access and blend information stored in common data distribution platforms such as Hadoop and NoSQL. Operators can leverage a graphical extract-transform-load tool to aggregate a uniform picture of desired information from a variety of sources – including image and video files – that is ready for analytical processing[13].

Existing Nationwide Data Standards

- Federal Bureau of Investigation, Criminal Justice Information Services (CJIS) Security Policy – The CJIS Security Policy has established federal requirements and agreements for creating, transmitting, and storing critical law enforcement records such as name, date of birth, and address.

[9] http://usc-isi-i2.github.io/karma/
[10] https://youtu.be/nlYCjSppPMU
[11] https://www.talend.com/products/data-integration
[12] http://www.jonathanlevin.co.uk/2008/03/open-source-etl-tools-vs-commerical-etl.html
[13] http://www.pentaho.com/product/data-integration

Analytics at the Edge – The working group foresees that industry will primarily be interested in improving the reliability and analytical capabilities of IoT devices and environmental sensors.

- Cisco – Cisco has developed a suite of "Analytics at the Edge" software for routers including: Connected Analytics for Events; Retail; Service Providers; IT; Network Deployment; Mobility; Collaboration; and Contact Centers.[14]
- Predixion - 'Predixion software, Predixion Insight 4.5 enables analytics to run on a device, on a gateway, and in the cloud. The tool is 'uniquely suited for IoT implementations due to its patent-pending Machine Learning Semantic Model (MLSM) technology which provides "predict anywhere" flexibility – the ability for advanced analytic packages to be embedded directly into a variety of production environments, including applications, databases, complex event processing engines, or even directly onto a connected or disconnected device.'[15]
- Dell – Dell Statistica is a middleware solution that allows for analytics on the gateway. Partnered with the Dell Edge Gateway 5000 Series, …the new hardware/software combination will provide faster local insights, and a reduction in data traffic to the cloud.[16]

Data Visualization

- Tableau – Tableau provides desktop, mobile, and cloud-based data visualization of big data. Tableau's Data Engine enables ad-hoc analysis of data. Tableau also enables users to blend disparate data sources through joining tables on a visual canvas. [17]
- Bair Analytics – Bair's Automated Tactical Analysis of Crime (ATAC) Workstation provides crime pattern analysis, predictive analytics, crime mapping, and report to crime investigations and intelligence analysis. ATAC assists analysts in pattern identification, data mining, analysis and prediction of serial events and communicating vital information. [18]

[14] http://www.datacenterknowledge.com/archives/2014/12/12/cisco-intros-edge-analytics-software-for-routers/
[15] https://www.predixionsoftware.com/News/ID/126/Predixion-Software-Takes-Advanced-Analytics-to-the-Edge-for-the-Internet-of-Things-Market
[16] http://www.forbes.com/sites/moorinsights/2015/10/21/can-dell-make-analytics-at-the-edge-a-reality/#12f310aa2758
[17] http://www.tableau.com/products/desktop
[18] http://www.bairanalytics.com/software/atac/

Public Safety R&D Opportunities

What project ideas should Public Safety R&D organizations consider as they prioritize upcoming investment opportunities?

Given the technology capabilities, gaps and barriers, and enabling action and actors that are forecasted to impact the analytics domain over the next 20 years, the Analytics Working Group identified several potential R&D efforts that would enable the integration of multiple data sources for the public safety community through enhanced analytics. Public Safety R&D organizations should consider the following project areas as they prioritize upcoming investment opportunities:

- Define common Public Safety (IoT data standards and processing models for specific public safety support activities.
- Collect IoT data integration software requirements for specific public safety support activities.
- Map which IoT data sources support common public safety operational tasks.
- Test for National Information Exchange Model (NIEM) compliance and Web 3.0 compatibility when developing common data standards and exchange protocols.
- Perform a gap analysis between disparate databases public safety projects to use to identify the compatibility errors and degree of inconsistency or inaccuracy incurred when merging these datasets. Estimate the time and cost required to resolve data integrity issues.
- Conduct pilot programs for commercially available data integration platforms in public safety settings and provide feedback on improvements to vendors and public safety end-users.
- Establish a standards-based software analytics framework to integrate and process disparate data sources.
- Conduct trade studies with industry and academia to gauge available data integration systems' suitability in public safety settings.
- Establish an IoT software certification process to drive public safety data standards and streamline the integration of public safety devices.
- Develop and promote software interface that promotes interoperability across public safety IoT devices.
- Develop "tripwire" software that triggers an alert due to analytic model results meeting or exceeding some threshold of risk or probability.
- Collect public safety requirements for a visual data integration user interface.
- Review existing data standards in industry that meet public safety requirements before developing unique public safety data standards.
    - Define which industry data standards fail to meet public safety requirements and identify what needs to be done to bridge the gap.
- Conduct use case study that identifies mission areas in which there are weak or nonexistent public safety data standards.
- Develop a nationwide compendium of data sources that are available and unavailable to public safety.
- Develop a software development guide on how to integrate externally available data sources with public safety-owned databases.
- Create a national, regional, or statewide "Information Sharing and Analysis Center" specifically for public safety use. The platform could operate similarly to data.gov but with public safety security and authentication requirements.

Data Governance & Golden Source Information

- Establish a federal certification body for validating golden source information available to public safety.
- Support future golden source certification processes evolve to accommodate new technologies and data structures.
- Establish public safety grade confidence thresholds for data integrity and reliability.
- Establish public safety grade time parameters for data integrity and reliability.
- Publish a series of certified golden source databases related to utilities, fixed infrastructure, biometrics, FAA airspace records, criminal history, background checks, and/or weather.
- Establish a standard for video indexing to be shared across public safety agencies and implemented in video analytics software.

Other

- Develop application brokers or lightweight middleware to translate, sort, and clean disparately structured data before analytical processing.
- Specify a standard in-vehicle computational platform to enable higher-fidelity analytics in mobile first responder software and hardware.
- Define standards and parameters for multi-variable control software.
- Develop open source algorithms to assist with analytics performed on ingesting data received at PSAP or other centralized public safety information centers.

Operational Objective: Analytics Improving Public Safety Data Processing

Data Processing refers to software's ability to conduct analysis on source data, build models, test and evaluate the accuracy of these models in a way that provides actionable insights for its users. These tools and techniques are used to extract useful information from data, and apply scientific methods to solve interdisciplinary, practical problems. Often data processing systems are built through a combination of computer programming, statistical experimentation, and machine learning. In commercial industry, advances in data processing and data science have revolutionized the way organizations recommendation products in online retail, identify fraudulent credit card transactions and execute asset trading on Wall Street, recommend new musical artists, and prioritize emergency calls.

In public safety settings, analytics software that enables more efficient, timely, and accurate data processing could assist in virtually any aspect of agency operations. Take for instance software analytics, which could diagnose a faulty algorithm that consume too much data or power, and could therefore leave a first responder stranded without connectivity if not addressed. Audio analytics would allow PSAPs to contextualize 911 calls based on words or phrases mentioned to provide insight into clues, witnesses, and event severity. More sophisticated entity analytics could clearly define group affiliation of individuals based on government records, social media data, and communications to detect non-obvious relationships between individuals or entities. Sentiment analysis could assess what these groups are talking about or concerned with. Whatever the objective, public safety has the opportunity to leverage the technological methods underlying these applications to more accurately predict emergency events, take action to prevent them, and respond more effectively when they occur.

Enabled Operational Capabilities

The Analytics Working Group identified three primary operational capabilities that would benefit from R&D focusing on enhancing public safety's ability to process data more efficiently and effectively. These include:

- Improved Situational Awareness
- Improved Decision Making
- Improved Information Management & Data Triage
- Improved Network Analytics

Technology Capabilities, Gaps, and Barriers

The Analytics Working Group identified several priority technology gaps that need to be addressed before public safety can begin exploiting analytics to improve the speed, efficiency, and accuracy of its data processing models. These gaps and the technology capabilities with which they are associated are listed in Table 4 below. One common theme present in many of these gaps is the need for public safety to more comprehensively understand the "state of the art" of analytical processing languages, tools, and programming techniques. This will help public safety understand the strengths, weaknesses, and relative tradeoffs of the data processing technologies available in terms of bandwidth, power, and memory requirements; and make more informed decisions on how to design analytic systems that meet different mission-critical and non-critical requirements. Given the wide variety of data processing options available in the market today, public safety agencies will need to more clearly define how mission and operational requirements align with the capabilities of potential analytics solutions before evaluating, procuring, and/or developing data processing systems within the agency.

1. Public safety realizes improvements in software's ability to process large, real-time data streams.

Developing software that can triage and process real-time streaming information in a timely, efficient matter is a critical technology enabler for improving the speed and effectiveness of emergency response. Stream processing has been used by financial institutions to automate sales & trading processes, telecommunication providers to monitor real-time quality of service data, and by municipalities to conduct real-time traffic analytics. Given that emergency response is a dynamic, and often reactionary exercise, public safety will need analytic solutions that can process high-velocity volumes of big data quickly so that they can react to changing response conditions in real time. Within the context of public safety, valuable data streams may include video or social media feeds, 911-call audio and texts, map layers, and changing weather conditions. If public safety were able to detect patterns from this real-time information, responders could evaluate the severity and geographic radius of a variety of incidents more quickly and accurately.

The Analytics Working Group forecasts that public safety will realize significant improvements in stream processing and streaming analytics in the next 5-10 years. Stream processing software seeks to analyze high-throughput data streams from sensors or dynamic databases by using "continuous queries" that operate over the duration of a given event. Improvements to the statistical models that enable analytics on the fly will allow public safety to process inbound data while it is in transit (rather than today's prevailing model of indexing and storing data before analytic processing). Public safety will also design stream processing system architecture to connect with external data sources (i.e. social media feeds and meteorological forecasts) to incorporate relevant information into application workflows[19].

Gaps & Barriers
Processing power needed for data triage of large, continuous data streams.
Analytics software needs ability to distinguish behavior or sentiment from unstructured or streaming data sources.
Need improved image matching capabilities and interoperability across devices and networks.
Need ability to generate automated alerts or actions based on rules, machine learning, or artificial intelligence software.
Push-based data visualization software is not currently used in public safety settings.
Challenge of integrating streaming data with existing database architectures.
Lack of querying mechanisms optimized for streaming, such as SQL on Streams (StreamSQL), used to find output events or compute real-time analytics on public safety applications.
Lack of scalable storage architecture that expands as the size of streaming data feeds approach public safety storage capacity limits.
Need to build software interfaces that allow public safety systems to seamlessly connect and communicate with external databases.

[19] http://www.infoq.com/articles/stream-processing-hadoop

2. Further advances in social media analytics software enables the improved processing of individuals' multimodal attributes, sentiment, and other features.

Social media analytics are commonly used today by businesses looking to mine their customers' sentiment and behavioral patterns for insight into their marketing and customer service operations[20]. Although detecting purchasing patterns may not have direct application to emergency response, the Analytics Working Group sees the practice of aggregating and processing data from websites, blogs, and social media accounts as becoming more popular and effective in public safety agencies over the next five years. One of the earliest applications of social media analytics in public safety is projected to be matching names used on social media accounts to physical attributes such as face and tattoos image data stored in one's profile. Law Enforcement will leverage social media data to deploy additional resources to areas of repeated crime activity, and integrating social media entries into private databases such as weapons registration, pharmaceutical purchases, or credit card processing records.

Other potential applications of enhanced social media analytics identified by the working group include integrating social media profile pictures into computer-aided dispatch (CAD) systems, and command and control centers conducting sentiment analysis on real-time social media feeds. Effective use of social media analytics is dependent on public safety developing data taxonomies "to filter and categorize the unstructured text found in social media.[21]" By leveraging statistical taxonomies, public safety information centers will gain the ability to organize and classify social media by topic or sentiments such as "gang activity," "violent crime," or "vulnerable infrastructure." These categories will provide public safety with greater visibility to the range and severity of threats posed to specific communities.

Gaps & Barriers
Vast majority of social media content does not contain reliable geolocation information.
Techniques for cross-referencing disparate data types are immature or not well understood in public safety contexts.
Need to integrate social media sentiment analysis with Natural Language Processing to more accurately interpret the intended meaning of social media chatter.
Need to define how and when public safety accesses social media data. Data retention and data custody processes are undefined.
Need to prioritize social media based on the content, user information, image, geolocation data associated with each record.
Public safety does not consistently leverage social media application program interfaces (APIs).

[20] http://searchbusinessanalytics.techtarget.com/definition/social-media-analytics
[21] http://www.sas.com/en_ca/insights/articles/analytics/public-safety-social-media.html

3. **Public safety increasingly leverages "state of the art" big-data processing languages, libraries, and techniques to increase the computing power, efficiency, and speed of their analytical systems.**

In order to accommodate the exponentially increasing amount of structured and unstructured data at their disposal, public safety systems will need to build their systems using programming languages that are optimized for specific data processing tasks and computing efficiency. For example, by building systems that use several languages such as Hadoop (which features considerable computing power necessary for analyzing large, disparate databases) and SQL (which uses query optimized techniques to increase data processing speed for certain types of data), public safety could perform analytics with speed and power that meet mission requirements[22]. Public safety is expected to gain a better understanding of which analytics languages and programming libraries outperform others in areas such as web scraping, database connections, statistical analysis, and visualization.

Adopting SQL-on-Hadoop, integrated R and Python analytics pipelines, and other "best of breed" systems that leverage the relative strengths of various big data processing languages will help public safety accommodate for hardware-based limitations on analytics (such as a handheld device's processing power) and interoperability concerns that arise when applications try to access data from different database structures. When considering the adoption of open-source programming libraries and techniques, public safety must ensure that these systems meet mission-critical cybersecurity requirements. Also, although open source techniques will likely meet public safety technical needs, existing government regulations and/or certification processes may slow adoption of these technologies in the short-term.

Gaps & Barriers
Currently public safety hardware does not have the processing power to perform big-data analytics locally on the device.
Public safety agencies need more education on "state of the art" analytics software languages, techniques, and libraries.
Need for consistent search methods for efficient filtering and classifying of large data sets.
Prevalence of siloed and independent databases in public safety agencies.
Need better ability to store, normalize, and share information collected through public safety sensors and CAD systems.
Public safety agencies need more ubiquitous and uniform access to data sources and open source programming libraries.
Need better ability to triage and process streaming data in transit or at the edge, rather than in a centralized location.

[22] http://www.asee.org/documents/zones/zone1/2014/Student/PDFs/215.pdf

4. Public safety begins dividing its analytical data sets into real-time and non-real-time to support improved prediction of response outcomes and post-processing activities.

Given the bandwidth constraints likely to come into play as a result of public safety processing larger, more frequent data inputs, emergency information centers will seek to define which data sources are mission-critical and need to be captured and processed in real-time. If public safety collects all data on a time response spectrum and catalogues the time response profile of data sources as they are collected, public safety will gain valuable insight into which data sources need to be "real-time" and which pieces of information are less time sensitive. After determining how often certain data sources need to be refreshed, public safety can prioritize bandwidth for mission-critical information, and build a reliable software schema that evaluates data quality vs. prioritization vs. bandwidth considerations vs. user connectivity. The Analytics Working Group anticipates that the public safety community will work together to develop a common understanding of how to balance these data tradeoffs for specific support functions. Improved database analysis software will assist public safety in determining how frequently and in what ways data sources change during normal operations, emergency situations, and post-event processing.

Gaps & Barriers
Lack of common standards and processing models for specific public safety support activities.
Ability to process and distill source data into meaningful outputs and predictors for operational personnel.
Need to define requirements and standardized processing models for mission-critical data.
Need to define requirements for real-time data, which data sources are needed in real-time, and whether "real-time" is a key characteristic for mission-critical data.
Existing public safety networks cannot accommodate bandwidth requirements for streaming real-time data.
Define data quality standards for what resolution and refresh rate will meet mission needs for specific operational tasks.
Need improved ability to prioritize processing bandwidth requirements for data that needs to be high quality.

5. Public safety begins adopting chain-of-evidence software systems to assist in data management.
Similar to a document management system, public safety data management platforms need to feature check-in, check-out, and versioning functions for all records used by analytical workflows. Any data or record that is input, derived, or changed must be documented and preserved so that public safety's analytics processing pipelines are manipulating accurate information. The Analytics Working Group projects that public safety will adopt a distributed revision control system similar to Git[23] – the most widely used source code management system for software developers today – to ingest and commit record updates and changes to the master public safety information center. A system similar to Git could assist public safety in managing and merging mission-critical records such as geolocation positioning and damage assessments during response. To enable improved data management, public safety will likely leverage inter-related databases and modeling software that allows for searching, meta-tagging, and auditing any changes to verified master records.

Gaps & Barriers
Need for improved analytics for cybersecurity and authentication to better manage and update master public safety records.
Need automated bandwidth management system to evaluate when it is feasible to sync local and master public safety records.
Need software that enables searching, meta-tagging, and auditing on local and master databases.
Need algorithms to perform cross evaluation or hypothesis testing that sets a confidence value on the reliability of analytical model or data source.
Need improved data compression algorithms to facilitate efficient data transport while maintaining data utility.
Difficult to process unstructured data such as audio or video without adding unnecessary or harmful "noise" and interference.

[23] https://git-scm.com/

6. Mobile security analytics capabilities will continue to mature and increase in importance.

The Analytics Working Group envisions that public safety organizations will prioritize developing more sophisticated analytics related to endpoint protection and data obfuscation. Given the sensitivity of information public safety will input into analytical systems, public safety will increasingly adopt analytics solutions that establish cybersecurity risk thresholds and deliver alerts via mobile devices when suspicious activity or threats are detected on their networks. Threat Intelligence software and security analytics will also become more ubiquitous at various levels of edge computing as public safety seeks to improve the resilience of IoT devices used in operations.

Gaps & Barriers
Security Analytics backend capabilities that extend beyond endpoint monitoring is a relatively new, non-researched area.
Need more sophisticated threat detection systems to minimize public safety network infiltrations.
Security Analytics need to minimize false positive and false negative threat detection readings.
Security Analytics software's reliance on high-speed data networks.
Definition of "public safety grade" or "mission-critical" analytics needs to include security requirements.
Public safety needs alternative ways to access and authenticate software in situations that are not conducive to typing, fingerprint scanning, or voice recognition.

7. Emergence of web-based analytics platforms make it easier for public safety agencies to process information and pilot analytics initiatives in the short-term.

Data analytics processing can be done in a variety of environments and with a wide variety of tools. Lightweight web-based analytics suites have become ubiquitous in recent years and allow organizations to experiment with analytics without significant sunk costs and time investments looming overhead. The working group anticipates that early analytics adopters in public safety will coalesce towards a common, web-based operational interface for data processing given the variety of platforms available today. These analytics suites will likely be first used for common, specific public safety support tasks such as crime mapping, fire risk assessment, and response route planning before becoming integrated with other organizational functions. Web-based analytic interfaces must be equipped with appropriate security and interoperability capabilities in order for public safety to connect their tools to external databases and devices. One of the principal challenges preventing organizations from pursuing more advanced analytics is that it is difficult to define specific problems to be solved.

Gaps & Barriers
Need to define how to expand on or consolidate overlapping, duplicative systems.
Lack of public safety grade device and information security analytics.
Public safety agencies need to more clearly define the objectives and "problems to be solved" by web-based analytic platforms.

Enabling Actions & Actors

What's being done? Who's doing it? How will remaining gaps and barriers be addressed?

This section is not intended to serve as an exhaustive review of all actions and actors supporting public safety's ability to improve its data processing capabilities. Rather, it is intended to provide a brief sample of R&D efforts both inside and outside of the public safety sector that represent the partnerships that public safety R&D organizations could build. Continued market research will be necessary to create awareness of current efforts and account for new actors in these fields.

Stream Processing

- Google Cloud Platform – Google's Cloud Platform provides an infrastructure to consolidate data streams from millions of connected devices, handles data ingest, processing, storage, and analysis of hundreds of millions of events per hour[24]. Although Google Cloud's data pipeline can perform analytics on data in transit (while streaming), most of the platform's analytical processing happens after records have been aggregated, transformed, and stored in cloud databases.
- Apache Spark – Apache Spark is an open source data processing engine that support machine learning on streaming data. Developers can build data streaming analytic applications in Java, Scala, and Python through Apache Spark's language-integrated API. Apache Spark's stream processing is commonly used for Twitter analytics and has been deployed at Yahoo! for personalizing news pages for specific users and optimizing digital advertising[25].
- IBM Streams – IBM's Streams analytics platform enables user-developed applications to ingest and analyze data in real-time from thousands of streaming sources[26]. IBM Streams can be integrated with Apache Spark applications and analytics and offers an open-source project on Github[27].

Social Media Analytics

- Purdue University, Center for Visualization and Data Analytics – In partnership with the Department of Homeland Security (DHS) Science and Technology Directorate (S&T), Purdue University developed the *Social Media Analytics and Reporting Toolkit* (SMART)[28]. This system uses topic extraction, word filter, and clustering techniques to visualize social media posts during an emergency scenario on an interactive map. SMART compares Twitter, Flickr, and YouTube data during events such as natural disasters, terrorist attacks, and traffic to historical data from similar past events. The Ohio State Highway Patrol and U.S. Coast Guard have tested SMART.

[24] https://cloud.google.com/solutions/architecture/streamprocessing
[25] http://www.datanami.com/2014/03/06/apache_spark_3_real-world_use_cases/
[26] http://www-03.ibm.com/software/products/en/ibm-streams
[27] https://github.com/IBMStreams
[28] https://www.dhs.gov/publication/improving-disaster-response-and-recovery-social-media-analytics-and-reporting-toolkit

- Esri and Geofeedia – Esri and Geofeedia offer an ArcGIS platform that enables Public Safety personnel to "integrate, analyze, and visualize live emergency data as events unfold.[29]" This application integrates social media feeds from Twitter, Instagram, Flickr, YouTube, and Google Photos with geolocation data including street networks and topography.
- Snaptrends – Snaptrends provides location-based social media analytics that include automated sentiment and trend analysis. Snaptrends has built a platform that monitors social media networks for law enforcement by placing a geofence around an area of interest and monitoring for keywords and images related to potential crimes[30].

Mobile Security Analytics

- Elasticsearch ELK Stack – As part of the Elastic Stack suite of tools, commercial extensions "Shield" and "Watcher" serve as security and alerting functions. "Shield" protects the entire ELK stack with encrypted communications, authentication, role-based access control, and auditing. "Watcher" is the alerting and notification product for Elasticsearch. It proactively monitors and alerts for anomalies in logs.[31]
- Splunk – Splunk provides a range of security-related products including Log Management, Enterprise Security, User Behavior Analytics, Advanced Threat Detection, and Insider Threat Detection.[32]

Public Safety R&D Opportunities

What project ideas should Public Safety R&D organizations consider as they prioritize upcoming investment opportunities?

Given the technology capabilities, gaps and barriers, and enabling action and actors that are forecasted to impact the analytics domain over the next 20 years, the Analytics Working Group identified several potential R&D efforts that would enable improved analytical processing in public safety. Public Safety R&D organizations should consider the following project areas as they prioritize upcoming investment opportunities:

Stream Processing & Analytics:

- Pilot test programs that use querying languages to process real-time data streams.
- Design scalable data storage architectures to be used in PSAP or other public safety data centers.

Social Media Analytics:

- Conduct comparison study between unique public safety data storage requirements, federal standards, and social media licensing agreements.

[29] http://www.esri.com/esri-news/releases/13-2qtr/esri-and-geofeedia-expand-social-media-with-location-analytics

[30] http://snaptrends.com/social-media-for/law-enforcement/#Snaptrends-for-Law-Enforcement

[31] https://www.elastic.co/products

[32] http://www.splunk.com/en_us/solutions/solution-areas/security-and-fraud.html

- Develop public safety community guidelines on how to collect and aggregate social media data from individuals.
- Develop an application that can extract, triangulate, or estimate social media geolocation data and metadata from text, network estimation, or contextual hashtags.
- Develop CONOPS standards to promote public safety outreach via social media.
- Develop a software interface and CONOPS to support 911 via social media.
- Partner with R&D community to design tools that analyze physical attributes and multimodal biometrics in images.
- Define requirements for social media analytics user interface.
- Develop CONOPS crowdsourcing platform to aggregate social media data during emergency events.
- Explore a virtual operations support team (VOST) CONOPS where public safety end-users can request social media support.
- Explore how wireless broadband emergency alerts can be more consistently incorporated into social media.

Improved Use of "State of the Art" Processing Languages:

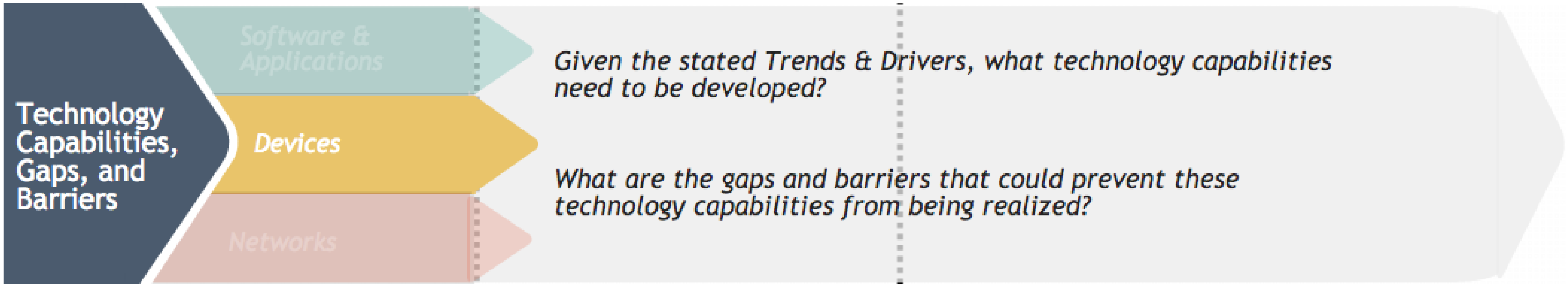
- Develop video scene processing and artifact identification standards.
- Establish methodology for determining cost-benefit and return-on-investment from deploying new analytics processing languages in public safety.
- Conduct experiments on how to integrate multiple cloud-based public safety networks to process data during times of network failure.
- Compare the processing, bandwidth, and power demands of similar analytic models written in different programming languages.

Other:

- Define data quality standards for specific public safety support tasks.
- Investigate how artificial intelligence can improve existing public safety algorithms and processing models.
- Establish a compendium of known correlations between data and predictors related to specific public safety support tasks.
- Drive NIST 800-124 and 164 adoption, testing, and revision of standards.
- Develop software analytics framework to integrate disparate data sources.

Security Analytics:

- Engage various network providers to identify how best practices in security backend analytics are applied in commercial networks, and how these best practices could be applied to public safety networks.
- Research inline security analytics techniques used across industry and academia.
- Develop security technologies that do not require a reliable connection to Internet backhaul such as local authentication and cyber defense systems.
- Design and integrate a cyber kill-switch to minimize risk of data leaks and theft on public safety applications.
- Investigate how to deploy automatic "honeypot" data that runs in sync with locally hosted data supporting analytical processes.

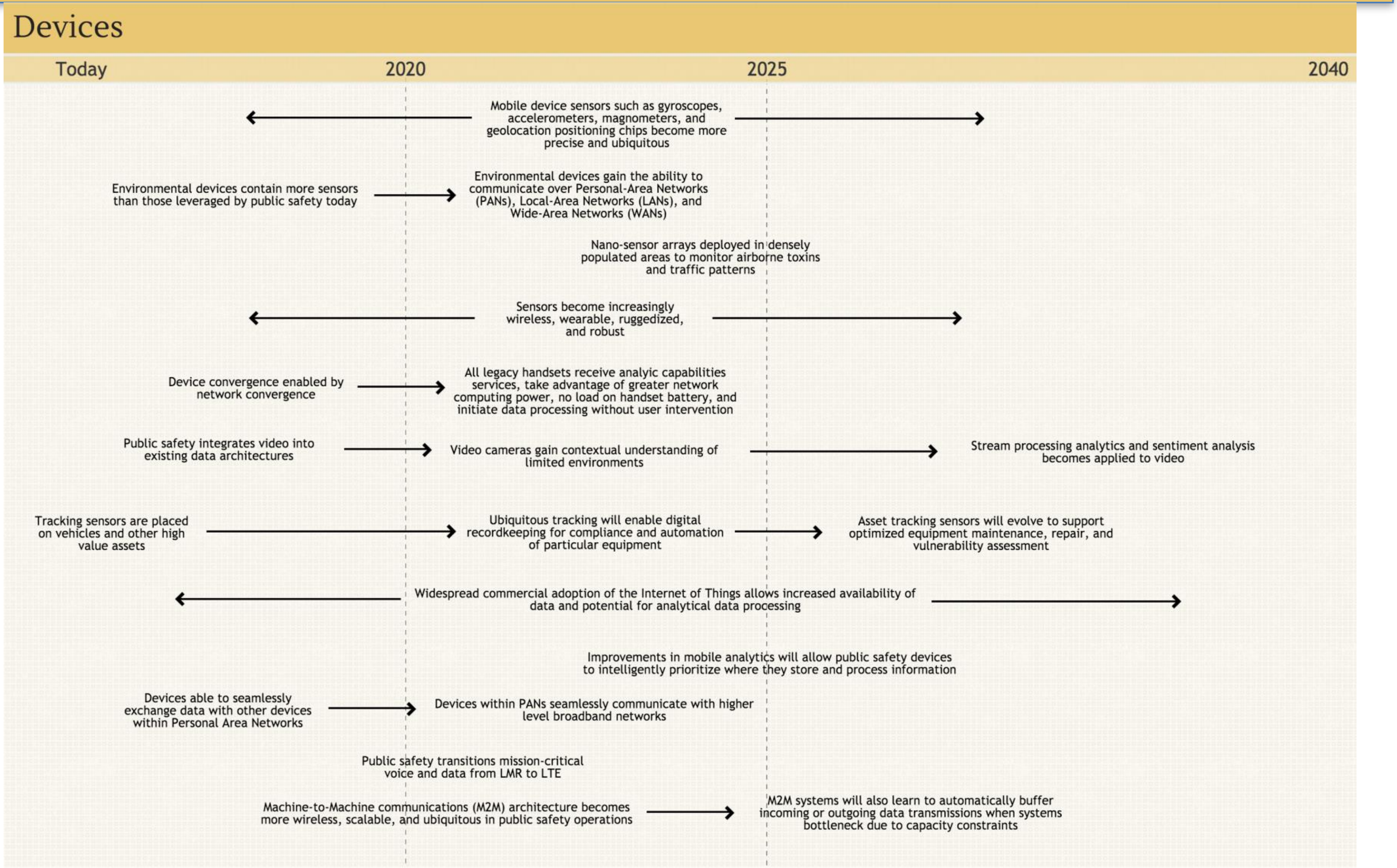

Technology Capabilities, Gaps, and Barriers
Software & Applications
Devices
Networks
Given the stated Trends & Drivers, what technology capabilities need to be developed?
What are the gaps and barriers that could prevent these technology capabilities from being realized?

Devices

Data-generating devices such as body-worn and environmental sensors, mobile handhelds, and ad-hoc server infrastructure will create vast data streams for public safety to improve their situational awareness, as well as operational and business decision-making. It has been well documented that industry and academia have invested significant financial and intellectual capital into commercializing the Internet of Things and Big Data Analytics, but these next-generation device capabilities need to meet mission requirements to become useful and adopted by public safety agencies nationwide.

After taking inventory of the variety of technical abilities, gaps, and challenges facing public safety's increased use of analytics-enabled devices over the next 5, 10, and 20+ years several themes became clear. Nearly all of the technology capabilities and gaps the working group identified in the Devices lane related to one of the following two operational objectives:

1. Devices serve to create, collect, store, process, and transmit data more effectively.
2. Devices serve as communications infrastructure and networks.



Devices

Today 2020 2025 2040

Mobile device sensors such as gyroscopes, accelerometers, magnometers, and geolocation positioning chips become more precise and ubiquitous

Environmental devices contain more sensors than those leveraged by public safety today → Environmental devices gain the ability to communicate over Personal-Area Networks (PANs), Local-Area Networks (LANs), and Wide-Area Networks (WANs)

Nano-sensor arrays deployed in densely populated areas to monitor airborne toxins and traffic patterns

Sensors become increasingly wireless, wearable, ruggedized, and robust

Device convergence enabled by network convergence → All legacy handsets receive analyic capabilities services, take advantage of greater network computing power, no load on handset battery, and initiate data processing without user intervention

Public safety integrates video into existing data architectures → Video cameras gain contextual understanding of limited environments → Stream processing analytics and sentiment analysis becomes applied to video

Tracking sensors are placed on vehicles and other high value assets → Ubiquitous tracking will enable digital recordkeeping for compliance and automation of particular equipment → Asset tracking sensors will evolve to support optimized equipment maintenance, repair, and vulnerability assessment

Widespread commercial adoption of the Internet of Things allows increased availability of data and potential for analytical data processing

Improvements in mobile analytics will allow public safety devices to intelligently prioritize where they store and process information

Devices able to seamlessly exchange data with other devices within Personal Area Networks → Devices within PANs seamlessly communicate with higher level broadband networks

Public safety transitions mission-critical voice and data from LMR to LTE

Machine-to-Machine communications (M2M) architecture becomes more wireless, scalable, and ubiquitous in public safety operations → M2M systems will also learn to automatically buffer incoming or outgoing data transmissions when systems bottleneck due to capacity constraints

Operational Objective: Devices Serve to Create, Collect, Store, Process, and Transmit Data More Effectively

The public safety community faces a tremendous opportunity to take advantage of advances in next-generation sensor technology for more creative and accurate analytic models. Significant commercial investment has already refined the precision of sensor readings, diversified their application, and made them more ubiquitous across industries like manufacturing, retail, and transportation. Although many of these next generation sensors have not yet been commercialized, the data that they create and transmit represent an untapped asset for public safety operational planning, resource allocation, and emergency response.

As sensors and machines produce vast data streams at varying levels of velocity, public safety will need to incorporate big data processing models such as Hadoop and NoSQL, and machine learning techniques into its communications architecture to transform real-time structured and unstructured data into more predictive decision-making[33].

Enabled Operational Capabilities

The Analytics Working Group identified three primary operational capabilities that would benefit from R&D focusing on enhancing public safety's ability to leverage devices that create, collect, store, process, and transmit data more effectively. These include:

- Improved Decision Making
- Improved Situational Awareness
- Improved Information Management & Data Triage

Technology Capabilities, Gaps, and Barriers

The Analytics Working Group identified several key technology gaps that need to be addressed before public safety can use its devices to create, collect, store, process, and transmit data more effectively. These gaps and the technology capabilities with which they are associated are listed in Table 5. One common, overarching technology gap that public safety must address is its readiness to triage data created with significantly increased volume and speed as a result of the Internet of Things and sensor ubiquity. Transporting this high-volume, high-velocity data will put undue strain on existing communications networks, so public safety must build more sophisticated analytic processing models locally on its own devices and interfaces to effectively cull meaningful intelligence out of data from 3rd-party sources. The proliferation of devices and sensors as data creation, processing, and decision-making centers also raise important interoperability concerns. The working group identified the need for additional standards development and requirements gathering to ensure the range of public safety devices can communicate effectively in this new environment.

[33] http://www.cloudera.com/content/dam/cloudera/Resources/PDF/Reports/TDWI_BPReport-Next_Gen_Analytics.pdf

1. **First responder devices contain more sensors than those in public safety operations today and will act as hubs for personal area networks (PANs).**

For the purposes of this operational objective, this section will focus on the proliferation of sensors on first responder devices and how these sensors are projected to enhance public safety decision-making. The working group anticipates that responder-worn devices will feature new, more sophisticated sensors to capture biometric and meteorological data in the short-term. The working group also envisions that public safety will be able to drive sensor development for specific public safety tasks, such as defining requirements for gas sensors that test air quality and levels of carbon monoxide, propane, and other gases during fire rescue. Public safety will also begin harnessing industry advances in mobile device sensors such as more precise gyroscopes, accelerometers, magnometers, and geolocation positioning chips on wearable communications devices. Although data created from these sensors will increase in quantity and resolution for the foreseeable future, public safety will need to design analytic systems to process this data on the device or on a PAN wearable to more efficiently manage bandwidth, power, and memory consumption when collecting or transmitting on-body data readings. Additionally, the PAN wearable could host data locally, so other end-users could access the data without the need for backhaul network communications. The PAN wearable could also support greater computation power than a mobile smartphone or sensor, thus reducing the need to send data over the backhaul communications for some analytics.

Gaps & Barriers
Computing power and memory available on existing devices.
Localized or personalized processing requirements for analyzing data being received from multiple and changing sensors as the location of the responder changes.
Moving analytics to the edge may conflict with existing incident command system architectures.
Insufficient ruggedization of commercially available sensors makes them unsuitable for many public safety response environments.
Need to develop data standards for on-body sensor readings.
Need for a standardized interface and interoperability across responder devices.
Need analytic systems to integrate information from responder devices within a given proximity to identify common threats during response.
Need for compression, storage, and file type standards for responder device data.
Difficult to anticipate the impact that on-body sensor analytics will have on existing Public Safety Concepts of Operations.
Need to design analytic systems to understand “normal” vs. “dangerous” biometric readings in the context of response activities.
Need to build in triggers and process controls into analytical systems that can alert, support, or shut down operations.
Need to develop Personal Area Network (PAN) standards to promote interoperability between individual devices, the PAN, vehicles, and a remote Command Center.

2. Environmental devices contain even more sensors than those leveraged by public safety today and will have the ability to communicate over PANs, Local-Area Networks (LANs), and Wide-Area Networks (WANs).

For the purposes of this operational objective, this section will focus on the proliferation of sensors on environmental devices such as IoT devices, closed-circuit television, and how these sensors deliver value to public safety decision-making. Similar to the sensors that are likely to become embedded with responder-worn devices, environmental device sensors will greatly increase in variety and data resolution. The working group anticipates that public safety will begin deploying submicro-sensor arrays in densely populated areas to monitor for airborne toxins that could detect bioterrorism or deteriorating critical infrastructure. Meteorological sensors that detect subtle changes in air pressure and wind direction with greater sensitivity will become commercialized in the next 5-10 years, so public safety – specifically fire and emergency rescue personnel – may have the opportunity to tap leverage existing sensor infrastructure or build their own to more accurately predict wildfires. The working group also indicated that sensors deployed on roads or traffic signals will likely monitor traffic patterns with greater accuracy and granularity, which could assist public safety with optimizing evacuation planning or prioritizing response routes. Over the next 20+ years, the environmental sensors available to public safety are anticipated to become increasingly wireless, ruggedized, and robust.

Gaps & Barriers
Limited battery capacity in environmental devices.
Lack of full-scale deployment of personal-area network technologies.
Need standardized network protocols to mitigate discovery and access challenges when communicating data over heterogeneous networks.
Lack of interoperability between commercially available environmental sensors.
Need to ruggedize commercially available environmental sensors to have high thermal, radioactive, and chemical particulate tolerances.
Forcing a set of stringent requirements on all sensors used by public safety will result in higher product cost and lower adoption rates.
Must design environmental sensors to operate without high-speed broadband connections, so that they can function inside and outside structures.
Need to determine how long to archive sensor data during and after an event.

3. Public safety integrates real-time situational sensors with video into emergency response.

Video camera technology is expected to increase in processing power, coverage area, and analytic sophistication in the medium- to long-term. Upgraded video sensor feeds could then be aggregated through sensor fusion and run analytical processes, which would enable the sensors themselves to possess contextual understanding of an environment. For example, an integrated video sensor network could identify and categorize suspicious objects that are of interest to public safety such as abandoned luggage, weapons, or disabled vehicles. By designing integrated sensor networks and video analytics systems that recognize and trigger alerts for specific objects or events, public safety agencies can respond more proactively in areas where these video sensors are deployed.

In the longer-term, the working group envisions that public safety's smart-video sensor networks will gain stream processing capabilities, so responders have the potential leverage video analytics in real-time as events develop. Public safety may also gain access to images, sound, and video from camera feeds not directly controlled by public safety; and successfully integrate these 3rd party video sources with public safety field devices.

Gaps & Barriers
Lack of interoperability between 3rd-party video feeds.
Feasibility of transmitting or integrating large video streams across wireless networks.
Need to develop video formatting standards.
Existing public safety databases may not be compatible with new data formats such as video or sensor data.
Current sensors carry a high cost of maintenance, upgrades, and replacement.
Sensors must be able to tolerate severe environments.
Limited ability to do image matching between video feeds and images in public safety databases.
Need to identify, manage, and track a wide variety of public safety devices without interference and jamming.
Need ability to conduct automated contextual video analysis in real-time.
Public safety unable to access and control 3rd-party video feeds.

4. **Public safety-owned device tracking becomes more common and accurate as a result of sensor proliferation.**

The working group envisions that small sensors that are either battery operated or energy-harvested will be placed on public safety assets with increasing frequency over the next 20 years. The ubiquity of devices possessing increasingly precise and reliable location-enabled sensors will significantly improve asset and compliance tracking. These sensors will enable digital recordkeeping for compliance and automation of particular equipment before, during, or after an emergency incident. In addition to geolocation tracking, asset-tracking sensors will evolve to support optimized equipment maintenance, repair, and vulnerability assessment.

Gaps & Barriers
Inability to connect sensors to personal area networks and local area networks.
Need to establish business rules for data collection and storage over time.
Sensors need intelligent interpolation/extrapolation capabilities to conduct analysis when network signals are not present.
Need improved cloud integration between sensors and cellular networks to enable asset tracking from mobile devices.
Need RF availability on-scene to enable personnel to transmit and receive data through various frequency bands.

5. **Widespread commercial adoption of the Internet of Things allows increased availability of data and potential for analytical data processing.**

The Internet of Things and data analytics are inextricably linked technologies, not only because the significant attention the two terms have received from all corners of the research community in recent years, but because sensor-embedded devices with a network connection ("things") will exponentially increase the volume of data eligible for analytic processing and the velocity with which it is created almost immediately[34]. Although estimates vary as to how many new IoT devices will be introduced over the next 20 years, network capacity constraints will force a significant portion of IoT data to be "stored, processed, analyzed, and acted upon close to, or at the edge of the network.[35]" To harness the data created from IoT devices, public safety can leverage advances in industry to develop analytic applications that plan device and network usage requirements during disaster situations, or optimize individual device performance and throughput given historical performance and environmental conditions during response[36].

Gaps & Barriers
Current data mining techniques need to be customized to IoT data.
Lack of standard interfaces for IoT devices.
Lack of spectrum for IoT devices.

[34] http://www.zdnet.com/article/the-internet-of-things-and-big-data-unlocking-the-power/
[35] http://www.idc.com/getdoc.jsp?containerId=prUS25291514
[36] https://infocus.emc.com/william_schmarzo/5-ways-the-internet-of-things-drives-new-opportunities/

6. LTE devices that serve as or connect to wearable sensors transmit, store, and analyze information.

As mobile devices begin running more complicated analytical processes that enhance situational awareness, collaborative decision-making, and prediction, public safety will need to overcome device limitations such as computational power, battery life, and reliance on high-speed network connections. Improvements in mobile analytics will allow public safety devices to intelligently prioritize where they store and process information based on factors such as available local memory, access to remote/cloud computing or storage resources, and application processing requirements[37].

Gaps & Barriers
Need for compression, storage, and file type standards for responder device data.
Need to map what analytic processes must occur at the edge vs. on the device vs. in a centralized location.
Need to improve transfer protocols development for securely exchanging files over LTE, short-range, personal, and other non-IP networks.
Need more efficient device charging technologies and battery life.
Need for more efficient data processing algorithms that consume less power.
Lack of sensor fusion and onboard processing for on-site, real-time data analytics.

7. Localized Analytics move closer to the actual collector and consumer of data.

One major capability repeatedly emphasized by the working group is the idea that of analytics “moving to the edge.” In the next five years devices such as smart phones, vehicle appliances, and PSAPs will all begin to complete analytical processes as they collect data in an effort to reduce the power, time, and capacity it takes to communicate actionable insights across a network connection.

Gaps & Barriers
Limited processing power internal to the device itself.
Biometric sensors need to capture and analyze a wide variety of multimodal attributes including iris, fingerprint, and facial recognition.
On-vehicle analytic systems may not be feasible due to the size, weight, and power requirements for necessary server architectures.
Need to define public safety requirements for localized/edge analytics.
Localized PSAP analytics require improved data governance procedures and processing models.

[37] http://www.journalofcloudcomputing.com/content/2/1/15

Enabling Actions & Actors

What's being done? Who's doing it? How will remaining gaps and barriers be addressed?

This section is not intended to serve as an exhaustive review of all actions and actors supporting public safety's ability to more effectively use devices to collect, store, process, and transmit data. Given the breadth of commercial, academic, and government activities relating to intelligent hardware development, environmental sensors, and the Internet of Things, continued market research will be necessary to ensure awareness for PSCR of current efforts and account for new actors in the analytics domain.

Improving the Quality of Mobile Sensors

- Apple – Apple has filed patents for the iPhone 7 that indicate that the device will feature sensors that can detect humidity, atmospheric pressure, temperature and ambient sound[38]. Although current iPhones have microphones that respond to direct audio input, these new sensors will enable the device to passively monitor and evaluate the surrounding environment.
- SensorDrone – SensorDrone has developed a suite of sensors that turns smartphones into a carbon monoxide detector, non-contact thermometer, lux meter, or proximity sensor. SensorDrone is an open platform that integrates sensor data with Android applications[39].

Improving the Quality of Environmental Sensors

- University of California, Riverside (UCR) – UCR has developed a nano-sensor that can detect airborne pathogens at a parts-per-billion resolution that is currently being commercialized by Innovation Economy Crowd (ieCrowd). The commercial sensor will be used to support products that can detect chemical warfare agents and trigger warning systems for bioterrorism[40].
- CLR Analytics, University of California – Irvine (UCI), US Department of Transportation (USDOT) – This public-private partnership is building a Next-Generation Traffic Monitoring System that improves on conventional traffic sensors. Today's traffic sensors merely provide volume, occupancy, vehicle presence and speed data. This project's goal is to build sensors that calculate more detailed information such as travel time estimates, vehicle classification, and origin-destination estimates[41].

[38] http://appleinsider.com/articles/14/04/24/future-apple-devices-may-boast-environmental-sensor-suite-with-built-in-thermometer

[39] https://stacksocial.com/sales/sensordrone-11-sensors-for-your-smartphone

[40] http://ucrtoday.ucr.edu/15913

[41] http://www.clranalytics.com/services/advanced-sensor-technologies

Public Safety R&D Opportunities

What project ideas should Public Safety R&D organizations consider as they prioritize upcoming investment opportunities?

Given the technology capabilities, gaps and barriers, and enabling action and actors that are forecasted to impact the analytics domain over the next 20 years, the Analytics Working Group identified several potential R&D efforts that would enable public safety devices to create, collect, analyze and transmit data more effectively. Public Safety R&D organizations should consider the following project areas as they prioritize upcoming investment opportunities:

- Define minimal user requirements, including security requirements, for responder-worn sensors and computing power needed to deliver on these requirements. Explore new low power Internet of Things security algorithms.
- Define data standards and exchange protocols for public safety-worn sensors.
- Define what a Personal Area Network means for public safety agencies.
- Develop an analytics framework for integrating disparate data sources across public safety devices and 3^{rd}-party devices and sensors.
- Research battery life advancements with academia and technology companies.
- Participate in Smart Cities initiatives sponsored by the White House Office of Science and Technology Policy (OSTP).
- Define public safety requirements for location resolution in a variety of common response environments.
- Identify requirements for public safety sensors across CONOPS and end-user needs.
- Develop public safety drone CONOPS in conjunction with the aviation safety community.
- Review advances in ultra low size, weight, and power (SWaP) Evolved Packet Core (EPC) and eNodeB technologies for wearable LTE devices.
- Develop technologies that enable multi-organizational access to asset tracking information.

IoT Analytics:

- Explore how bandwidth, latency, spectrum interference, and processing requirements change as a function of the number of devices active on a network.
- Determine how many additional devices existing commercial network protocols can handle without degrading performance.
- Conduct analysis on the particle use of Band 14 for IoT devices.

Operational Objective: Devices Serve as Communications Infrastructure

Public safety devices will see significant improvements in the way that they communicate with one another and with higher-level networks in the near future. Public safety will soon gain the ability to communicate data, analytical processing, and analytic results across a variety of device-enabled networks that helps support greater portability ("movable from place to place") and mobility ("usable when moving") of analytical systems[42]. Connected devices and interoperable heterogeneous networks will provide public safety with the ability to offload analytical processing to certain devices or networks – such as a responder's smartphone offloading analytic tasks to a smartwatch or vehicle nearby. Analytics will assist these machines intelligently prioritize which network band, processing location, and data quality levels need to be used to generate intelligence that meets mission needs.

The technologies enabling devices to serve as communications infrastructure include enhanced Machine-to-Machine communications, more sophisticated analytics within hardware, and more efficient in-memory computing that stores source data and conducts analytics within a server to increase processing and transmission speeds[43].

Enabled Operational Capabilities

The Analytics Working Group identified three primary operational capabilities that would benefit from R&D focusing on enhancing public safety's ability to leverage devices as communications infrastructure. These include:

- Improved Decision Making
- Improved Situational Awareness
- Improved Information Management & Data Triage
- Improved Network Analytics

Technology Capabilities, Gaps, and Barriers

As public safety devices gain the ability to create, sustain, and communicate with one another across their own area-networks, the responder community needs to anticipate how these new capabilities will be integrated or change existing Concepts of Operations. These heterogeneous network architectures will need greater ability to scale within a public safety agency and across jurisdictions to ensure interoperability during response. The working group identified the need for devices to possess improved data and network prioritization capabilities locally in its hardware as a technology gap that spanned across this operational objective. These gaps and the technology capabilities with which they are associated are listed in Table 6 below.

[42] http://www.computerworld.com/article/2483791/emerging-technology/what-wearable-computing-is-really-all-about.html
[43] http://www-01.ibm.com/software/data/what-is-in-memory-computing.html

1. **First responder devices contain more sensors than those in public safety operations today and will act as hubs for personal area networks (PANs).**

Although the working group identified this capability one that supports devices creating and collecting data, for the purposes of this operational objective, this capability will focus on how first responder devices will act as hubs for personal area networks. As public safety begins to integrate more wearable connected devices into daily operations in the coming years, these devices will gain the ability to seamlessly exchange data with other devices within the PAN. In addition to communicating locally, these devices will connect to an Internet or broadband-enabled mobile device – most likely a smartphone or some iteration thereof assuming the role of IP server – to relay data collected and processed within the PAN to centralized public safety analytics centers through higher level networks. This will enable public safety to balance capacity constraints and processing demands between heterogeneous networks, so that mobile analytics tools remain reliable in times of high network traffic or data throughput.

Gaps & Barriers
Computing power and memory available on existing devices.
Localized or personalized processing requirements for analyzing data being received from multiple and changing sensors as the location of the responder changes.
Moving analytics to the edge may conflict with existing incident command system architectures.
Insufficient ruggedization of commercially available sensors makes them unsuitable for many public safety response environments.
Need to develop data standards for on-body sensor readings.
Need for a standardized interface and interoperability across responder devices.
Need analytic systems to integrate information from responder devices within a given proximity to identify common threats during response.
Need for compression, storage, and file type standards for responder device data.
Difficult to anticipate the impact that on-body sensor analytics will have on existing Public Safety Concepts of Operations.
Need to design analytic systems to understand “normal” vs. “dangerous” biometric readings in the context of response activities.
Need to build in triggers and process controls into analytical systems that can alert, support, or shut down operations.

2. Mission critical voice and data processing occur on a single device.

The working group believes that more sophisticated device analytics will enable public safety to process and transmit mission critical voice and data on the same device in the next 5-10 years. Specific capabilities that were identified by the working group include speech recognition for talk to text, speaker identification, and verification to authenticate specific users. In order to transition mission critical voice and data from LMR to LTE, the public safety R&D community will develop more efficient simulation models to evaluate LTE device performance and sensitivity during times of high noise and specific emergency scenarios.

Gaps & Barriers
Need to develop speaker identification, verification, and speech recognition technologies on public safety LTE devices.
On-device recording and storage of communications transcripts may overwhelm LTE memory and processing capabilities.
Need to develop more efficient simulation models comparing the performance of LMR and LTE devices processing mission critical voice and data.

3. Machine-to-Machine communications (M2M) architecture becomes more wireless, scalable, and ubiquitous in public safety operations.

Effective M2M architecture was cited as a critical enabler for public safety's ability to conduct analytics on IoT devices and data feeds. The working group also indicated that public safety LTE devices will gain the ability to connect to mobile data terminals through secure, encrypted ad-hoc network connections (Wi-Fi, Bluetooth, LMR, cellular) to more effectively share data and intelligence across other devices used on-site or at Incident Command. Through enhanced analytics, M2M systems will also learn to automatically buffer incoming or outgoing data transmissions when systems bottleneck due to capacity constraints. M2M will become more intuitive and simpler for responders to control due to the development of user interfaces that control M2M devices such as wearable sensors, building controls, and CCTV systems.

Gaps & Barriers
Public safety M2M communications architectures need the ability to prioritize network traffic and buffer data transmissions so that bandwidth is optimized during peak usage.
Need to prioritize network traffic in light of mission requirements.
Lack of standards to interact with devices collecting and transmitting data.
Lack of conversion protocols for various device operating systems.
Need to enable automated M2M communications at the edge, without relying on central processing technologies.

4. Device analytics continue to evolve as an extension of the network.

The collection of information from local devices will necessitate lower level analytics – functions such as data filtering, aggregation, and cleaning – be done locally on the device. Higher-level analytics – functions such as statistical modeling and data visualization – can be executed on communications networks if local, device-based analytics continue to mature. System developers will need to understand the tradeoffs between where analytics occur and how this affects the data and information flow with respect to decision support. As device analytics mature and reduce the need to process all data on the network, public safety will improve its ability to determine how and where to distribute information and analytical processing to maximize efficiency.

Gaps & Barriers
Processing power and battery efficiency of public safety devices need to improve.
Need to define public safety on-body device requirements and standards, and engage industry to develop sensors that meet these requirements.
Devices need greater intelligence to know understand when it should offload some of its analytical processing to a nearby device if it is in danger of reaching capacity.
Need improved on-device communications prioritization.

Enabling Actions & Actors

What's being done? Who's doing it? How will remaining gaps and barriers be addressed?

This section is not intended to serve as an exhaustive review of all actions and actors supporting public safety's ability to more effectively use devices as communications infrastructure. Given the breadth of commercial, academic, and government activities relating to Machine-to-Machine communications and device analytics, continued market research will be necessary to ensure awareness for PSCR of current efforts and account for new actors in the analytics domain.

Machine-to-Machine Communications:

- The Department of Homeland Security (DHS), Balfour Technologies – DHS S&T is working to identify a scalable approach to using different networks to improve M2M communications for first responders. In partnership with Balfour Technologies, DHS S&T is investigating how to enable smart building devices to communicate with first responders through secure mobile M2M applications[44].

[44] https://www.dhs.gov/sites/default/files/publications/Machine-to-Machine%20Architectures%20to%20Improve%20First%20Responder%20Communications-M2M-508.pdf

- Aeris – Aeris is a service and technology provider specializing in end-to-end M2M and IoT services. Aeris offers a cellular network exclusively built for Machine-to-Machine communications[45].
- Commercial Network Carriers – Commercial network providers such as AT&T, Verizon, and Sprint have invested significant resources to improving the speed, reliability, and data throughput of M2M communications in preparation for 5th-generation wireless (5G) set to roll out in 2020. Enhanced M2M communications will be a key differentiator between 5G and current LTE networks, and these large carriers are currently driving M2M R&D in North America.
- LDLN – LDLN is a service and technology provider focus on providing the end-to-end framework for organizations to instantly communicate data during a disaster without the need for Internet, cell service, satellites, or phone lines. LDLN has partner with the Seattle Office of Emergency Management and the National Guard for exercises in Washington State since 2014.[46]

Public Safety R&D Opportunities

What project ideas should Public Safety R&D organizations consider as they prioritize upcoming investment opportunities?

Given the technology capabilities, gaps and barriers, and enabling action and actors that are forecasted to impact the analytics domain over the next 20 years, the Analytics Working Group identified several potential R&D efforts that would enable public safety devices to proliferate networks and serve as communications infrastructure. Public Safety R&D organizations should consider the following project areas as they prioritize upcoming investment opportunities:

- Define public safety grade standards for device-enabled Personal Area Networks.
- Develop public safety grade noise reducing codecs for both LMR and LTE voice quality.
- Define requirements (data processing, security, storage, etc.) for on-device recording and storing of communications transcripts.
- Develop scenario-based use cases to explore the feasibility and impact of Machine-to-Machine communications technology.
- Explore using device-embedded analytics to better manage (prioritization, bandwidth use, etc.).

[45] http://www.aeris.com/about-aeris/
[46] http://ldln.co/

Technology Capabilities, Gaps, and Barriers
Software & Applications
Devices
Networks
Given the stated Trends & Drivers, what technology capabilities need to be developed?
What are the gaps and barriers that could prevent these technology capabilities from being realized?

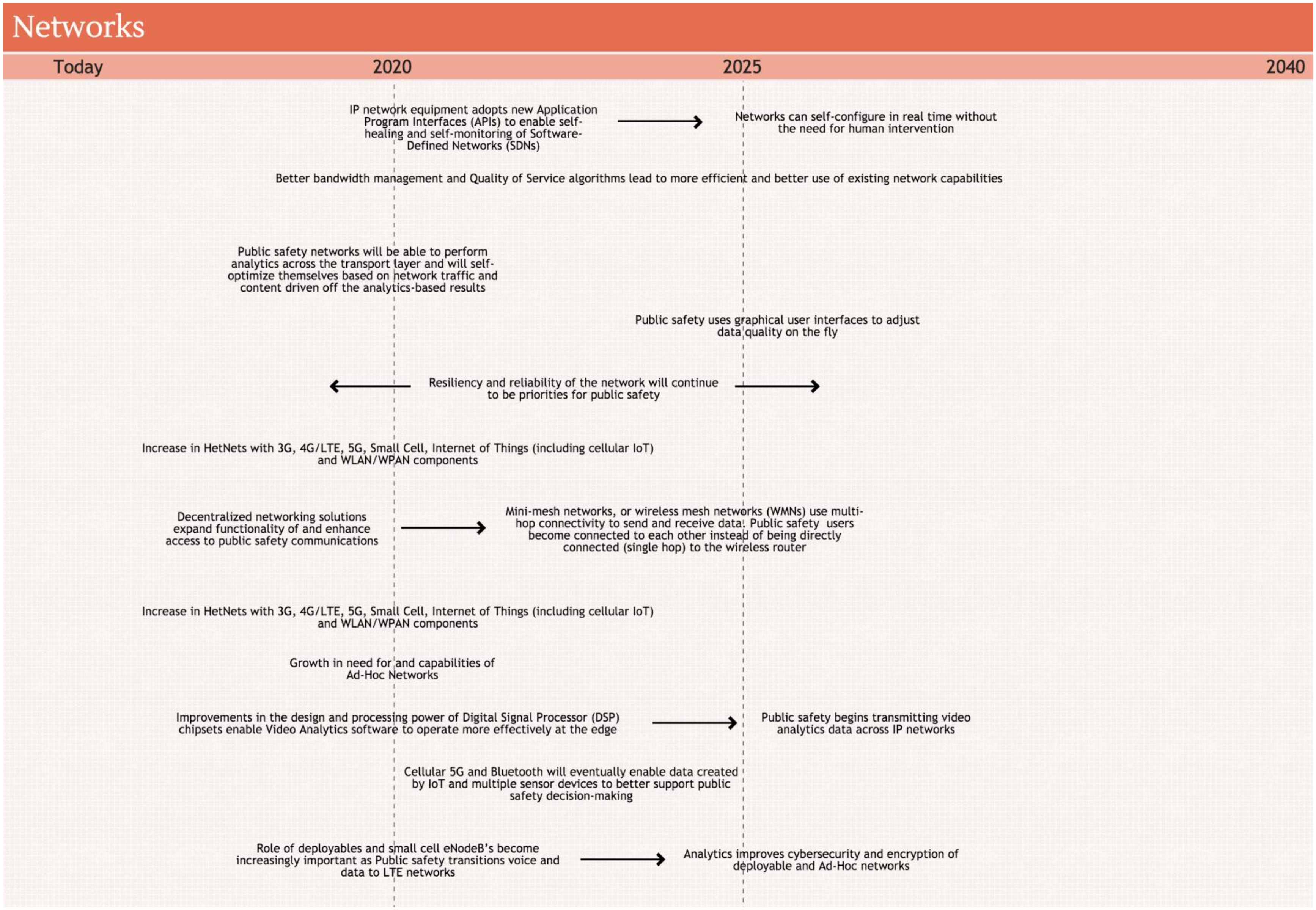
Networks

To effectively respond to emergency incidents nationwide, public safety requires inter-agency communications in a multitude of environments. Traditionally, public safety has relied upon LMR-based connectivity to their home jurisdiction's network, connecting to pre-arranged shared channels or talk groups with neighboring jurisdictions, or utilizing nationwide interoperability channels when responding far outside of their home jurisdiction. As the FirstNet network is initially built out, the network will not provide the significant coverage overlap and redundancy that exists in today's LMR environment. In the transition from LMR-based communications to an IP-based network capabilities will emerge that w enable public safety to leverage existing, newly created, and ad-hoc networks to complete mission-critical functions.

Fortunately for public safety, the move to IP and LTE-based networks enable first responders to benefit from technology advancements from a much broader industry base than the traditional LMR market. The Public Safety Analytics Working Group forecasted the evolution of numerous technology capabilities that, while meaningful and valuable for the public safety community, are priority efforts for other industries such as health, utilities, transportation, and the smart-home community. The Internet of Things (IoT) community will play a large role in helping public safety realize some of the most critical network-related technology capabilities discussed below. This confluence of stakeholders, industries, and markets can play an accelerating role in public safety achieving enhanced capabilities in the short, medium, and long-term.

As the Public Safety Analytics Working Group discussed the Networks lane, several operational objectives surfaced as natural themes that captured the collective technology capabilities and enabled operational capabilities. For the purposes of this report, two operational objectives have been discussed in detail:

1. Network Self-Optimization
2. Decentralization of Networks



Networks

Today | 2020 | 2025 | 2040

IP network equipment adopts new Application Program Interfaces (APIs) to enable self-healing and self-monitoring of Software-Defined Networks (SDNs) → Networks can self-configure in real time without the need for human intervention

Better bandwidth management and Quality of Service algorithms lead to more efficient and better use of existing network capabilities

Public safety networks will be able to perform analytics across the transport layer and will self-optimize themselves based on network traffic and content driven off the analytics-based results

Public safety uses graphical user interfaces to adjust data quality on the fly

← Resiliency and reliability of the network will continue to be priorities for public safety →

Increase in HetNets with 3G, 4G/LTE, 5G, Small Cell, Internet of Things (including cellular IoT) and WLAN/WPAN components

Decentralized networking solutions expand functionality of and enhance access to public safety communications → Mini-mesh networks, or wireless mesh networks (WMNs) use multi-hop connectivity to send and receive data. Public safety users become connected to each other instead of being directly connected (single hop) to the wireless router

Increase in HetNets with 3G, 4G/LTE, 5G, Small Cell, Internet of Things (including cellular IoT) and WLAN/WPAN components

Growth in need for and capabilities of Ad-Hoc Networks

Improvements in the design and processing power of Digital Signal Processor (DSP) chipsets enable Video Analytics software to operate more effectively at the edge → Public safety begins transmitting video analytics data across IP networks

Cellular 5G and Bluetooth will eventually enable data created by IoT and multiple sensor devices to better support public safety decision-making

Role of deployables and small cell eNodeB's become increasingly important as Public safety transitions voice and data to LTE networks → Analytics improves cybersecurity and encryption of deployable and Ad-Hoc networks

Operational Objective: Analytics Enabling the Self-Optimization of Networks

The transition of public safety communications networks from Land-Mobile Radio (LMR)-based systems to Internet Protocol (IP)-based systems will enable a host of new capabilities for designing and operating the network to meet public safety requirements. Public safety will have access to capabilities such as priority, quality control, and preemption. The *2012 NPSTC Public Safety Broadband High-Level Launch Requirements* call out some specific examples of network control and optimization that are particularly of interest to public safety:

- "The NPSBN SHALL be engineered to prevent traffic congestion at every stage of the network to meet NPSBN GoS objectives.
- The NPSBN SHALL support capacity and/or coverage expansion to address evolving user needs.
- The design of the NPSBN SHALL account for higher traffic demand in areas deemed strategic by FirstNet and/or Public Safety Entities."[47]

These are just a few examples of the capabilities enabled by IP technology. The PSCR Analytics Working Group further described additional technology capabilities that will allow not only for network control and optimization, but self-optimization that will occur automatically 'in the background' enabled by advancements in network-related analytics.

Enabled Operational Capability: Improved Network Analytics

The Analytics Working Group identified Improved Network Analytics as a critical operational objective of future R&D to support the public safety community. Specific to analytics, the main technology capabilities that arise from R&D directed at improving network analytics include:

Technology Capabilities, Gaps, and Barriers

The Analytics Working Group identified several key technology gaps that need to be addressed before self-optimizing networks can become a reality for public safety. These gaps and the technology capabilities with which they are associated are listed in Table 7 below. One theme present in many of these gaps is the need for public safety to define 'mission-critical data'. This definition has ramifications that will inform the development of analytical tools and capabilities, and enable network self-optimization. Understanding not only what data is considered mission-critical, but in which situations or scenarios is also key. Public safety may determine certain data is mission-critical for responding to a building fire, while an entirely different set of data is mission critical for responding to a flooding event or vehicle crash. Upon defining mission-critical data and establishing scenario-based mission critical data sets, the ability of the network to recognize mission-critical data vs. non-mission-critical data is a key gap to be addressed to enable network self-optimization.

[47] http://www.npstc.org/download.jsp?tableId=37&column=217&id=2609&file=BBWG_SoR_Launch_12112012.pdf

1. IP network equipment adopts new Application Program Interfaces (APIs) to enable self-healing and self-monitoring of Software-Defined Networks (SDNs).

"Software-Defined Networking is the physical separation of the network control plane from the forwarding plane, and where a control plan controls several devices… this architecture allows the network control to become directly programmable."[48] SDNs allow integration between the applications riding on top of a network and the underlying network infrastructure. The network can self-configure in real time without the need for human intervention. New applications can be deployed on top of the network infrastructure without the need for configuration or software/firmware updates for network elements. These capabilities will allow public safety to ensure optimal network operations in support of their communications requirements.

Gaps & Barriers
Leveraging SDNs requires new thinking – network engineers need to understand modern scripting languages and web-based APIs that are common in application development.
The concept of SDNs is very new and the standards and best practices are still emerging.
Few networks will be 100% software-defined from launch; most will gradually deploy SDN-enabled applications as knowledge and best practices are developed.

[48] https://www.opennetworking.org/sdn-resources/sdn-definition

2. Networks perform deterministic analysis on traffic patterns associated with bandwidth utilization and traffic types.

The proliferation of network data collection systems has resulted in an overwhelming flood of content. With data coming from many types of geographically-dispersed sources, the time it can take first responders and their supporting Public Safety and Federal partners to identify the actionable intelligence can be significant. In the near term, the Analytics Working Group believes that public safety networks will be able to perform analytics across the but not limited to the transport layer and will self-optimize themselves based on network traffic and content driven off the analytics-based results. In the longer-term future, the network will anticipate changes before they happen with a fair amount of certainty. Traffic types include, voice, data, video, priority levels, and delay characteristics. It will also optimize multiple, heterogeneous sources of data in the most network-efficient way possible. The network will be able to identify relevant data sources to public safety and determine how they can be integrated into an interoperable framework.

Gaps & Barriers
Need for market analysis to determine total addressable market to drive industry R&D investment.
Need increased data processing power of the analytic.
Public safety must define what “mission-critical data” is relative to their operational plans. The definition will depend on the context of a public safety agency. Without defining how it intends to use data, public safety cannot build the necessary infrastructure needed to manage the mission.
Network resiliency and prioritization services are needed to analyze mission-critical data when the network goes down or is overloaded from a bandwidth standpoint.
Need for interoperable data sources (data standards, APIs, or interfaces such as JSON, XML, etc.).
Lack of this data being resident on FedRamp certified cloud infrastructures.
Networks will need to self-optimize in response to damage to the network (both physical and cyber damage).
Need a network-based element that discovers critical pieces of content needed from disparate data sources across the public safety enterprise, and delivers them to public safety users. Need to create a standard and/or usage scenario that indicates what information or analytical capabilities are necessary during fire, flood, vehicle crash, etc.

3. Improved image/video/sound quality and the capability to enhance quality "on the fly".
Inherent to network self-optimization is the capability for network adjustments to happen "on the fly". This is particularly important to public safety where the need for improved video or audio quality may change from shift to shift or more immediately, from minute to minute. While it is anticipated that the first responder may have some ability to "turn the knob" through applications to manipulate image, video, and audio quality, the Analytics Working Group anticipates that some of these decisions may be able to be pre-determined or driven by analytics collected and processed from many different sources of information relevant to the event.

Gaps & Barriers
Need to ensure new technology is compatible with legacy systems. Needs to meet at minimum, mission-critical standards for LMR (e.g. audio quality).
Need to understand the data source (digital vs. analog) and conduct appropriate analytics to optimize the data type.
Need to avoid disposing of the original data source after making improvements to audio/video.
Bandwidth constraints – need to determine when it is operationally necessary to have maximum quality vs. when lower levels of quality may be sufficient.

4. Resiliency and reliability of the network continue to be priorities for public safety.
Resiliency to physical attacks, natural disasters, and cyber attacks will only grow as a priority for public safety networks. The ability of the network(s) to maintain resilient in the face of such attacks will largely depend upon the ability of the network to self-identify, self-diagnose, and self-heal/restore. Analytics will drive the ability of the networks to remain resilient and reliable under these attacks. Analytics will drive the ability of networks to identify and route traffic to alternate paths when a part of the network is damaged or down due to cyber threats. The Analytics Working Group recommended viewing the network as a holistic entity rather than as separate pieces, and to address vulnerability in the same holistic manner.

Gaps & Barriers
Need to understand the mission, available bandwidth, and data being communicated across the network in order to properly manage the tension between throttling/compressing content and the quality of data needed to accomplish the public safety mission.
Content owners need to prioritize certain data types over others and consider the most economical way of using bandwidth. Network Transport needs the flexibility to reprioritize on the fly. Need to consider precedence preemption when prioritizing these responsibilities.
Analytics that require significant bandwidth (video) will put significant strain on the network.
Need optimized techniques in load balancing across alternate routes to prevent overloading of congested links.
Need to better understand how analytics deal with communication networks that have been damaged by an emergency event. Similar to load balancing (i.e. using alternate paths when part of the network is down.).
Network reliability and resiliency need to be examined across the entire network. Need to identify potential chokepoints. Need to view the “network” as a holistic entity rather than as separate pieces. Also need to think about vulnerability holistically.
Auto detection – public safety needs a better understanding of their communications networks on a moment-by-moment basis. Networks need better situational awareness. Edge computing devices need to be able to report to the network whether or not they’re functioning and/or they’re connected to the network.
Analysis of wireless networks to route data through alternative paths due to network saturation or outages.
Prevention of wireless security attacks such as detecting rogue towers.
Analyze traffic patterns to discover potential attacks.

Enabling Actions & Actors

What's being done? Who's doing it? How will remaining gaps and barriers be addressed?

This section is not intended to be an exhaustive review of all enabling actions and actors currently working on self-optimizing networks related analytics efforts. Rather, it is intended to provide a brief sample of R&D efforts both inside and outside of the pubic safety sector that represent the partnerships that public safety R&D organizations could build. Continued market research will be necessary to create awareness of current efforts and account for new actors in these fields.

Self-Organizing & Self-Healing Networks

- Harris - Harris LTE networks include load management capabilities to automatically balance user demand and access in congested or high-load areas. With these network management tools, the Harris LTE network continues to support these mission-critical applications, even when first responders congregate to address major incidents.[49]
- Motorola - Hardened public safety LTE systems self-heal and autonomously reconfigure around network failures through Self-Organizing Network (SON) design while interoperability gateways will dynamically steer traffic to the best network based on performance and availability.[50]
- Nokia - Self-Organizing Network (SON) automation tools detect events like cell outages and activate automatic self-healing. Nokia distributed SON is based on 3GPP standards and the functionality is implemented in radio network elements. Distributed SON has a specific role especially in functionality that requires low latency and where centralized SONs would add unnecessary delay. Nokia distributed SON is also known as Nokia iSON.[51]
- Reverb – Reverb's InteliSON is a self-optimizing network command center. InteliSON identifies sites and cells that demonstrate certain failure/outage indicated by alarms from the fault management (FM) system of the OSS. Based on this feedback, it classifies cells as Outage Cells and attempts a series of antenna tilt changes to neighboring cells in order to restore service to the area affected by the outage.[52]
- XG Technology, Inc. – Cognitive Radio Networks for Public Safety Applications - the system uses Dynamic Spectrum Access technology to maximize throughput and reliability, delivering a licensed spectrum experience in unlicensed spectrum.[53]

Software-Defined Networks (SDN)

- Cisco – Evolved Services Platform, Application Centric Infrastructure for the data center, Evolved Programmable Network.[54]
- Big Switch Networks - Big Monitoring Fabric (BMF) enables pervasive security and monitoring of network traffic for an organization and selectively delivers it to multiple security, monitoring, and performance measurement and compliance tools.[55]

[49] https://www.nppgov.com//wp-content/uploads/Harris_VH10954_PublicSafety_LTE_Advantages.pdf
[50] https://www.motorolasolutions.com/content/dam/msi/Products/two-way-radio--public-safety/MOT_Beginning_of_the_Future_4G_WP_EN_101811.pdf
[51] http://networks.nokia.com/portfolio/solutions/self-organizing-networks
[52] http://www.reverbnetworks.com/products/
[53] http://www.xgtechnology.com/cognitive-radio-networks-for-public-safety/
[54] http://www.cisco.com/c/en/us/solutions/software-defined-networking/overview.html
[55] http://www.bigswitch.com/products/big-monitoring-fabric

- Open Networking Foundation - Open Networking Foundation (ONF) is a user-driven organization dedicated to the promotion and adoption of Software-Defined Networking (SDN) through open standards development.[56]
- OpenStack - The OpenStack Foundation promotes the development, distribution, and adoption of the OpenStack cloud operating system. The goal of the OpenStack Foundation is to serve developers, users, and the entire ecosystem by providing a set of shared resources to grow the footprint of public and private OpenStack clouds.[57]
- Open Compute Project - The Open Compute Project Foundation is a rapidly growing community of engineers around the world whose mission is to design and enable the delivery of the most efficient server, storage, and data center hardware designs for scalable computing.[58]

Public Safety R&D Opportunities

What project ideas should Public Safety R&D organizations consider as they prioritize upcoming investment opportunities?

Given the technology capabilities, gaps and barriers, and enabling action and actors that are forecasted to impact the analytics domain over the next 20 years, the Analytics Working Group identified several potential R&D efforts that would deliver enhanced self-optimizing networks to the public safety community based on improved analytics. Public Safety R&D organizations should consider the following project ideas as they prioritize upcoming investment opportunities:

- Perform a wide sector market survey to determine state-of-the-art data analytics capabilities, problems, and areas of research.
- Applied research for more capable software recognition and analysis capabilities.
- Develop network resiliency and prioritization services to enable mission-critical data when the network goes down or is overloaded from a bandwidth standpoint.
- Development of a network-based element that discovers critical pieces of content needed from disparate data sources across the public safety enterprise, and delivers them to public safety users. Create a standard and/or usage scenario that indicates what information or analytical capabilities are necessary during routine (house fire, vehicle crash, etc.) and extraordinary events (forest fire, flood, etc).

[56] https://www.opennetworking.org/about/onf-overview
[57] http://www.openstack.org/foundation/
[58] http://www.opencompute.org/about/mission-and-principles/

Operational Objective: Decentralization of Networks

As public safety adopts future generation communications technology, and data starts to become considered "mission critical", being able to decentralize network capacity and capability will enable public safety to continue mission critical functions as well as perform data analytics at the cell edge. Network decentralization also makes networks faster by regionalizing components of the core network like the Mobility Management Entity (MME) and Policy and Charging Rules Function (PCRF) and reducing backhaul requirements. Radio Access Networks (RAN) are also now able to manage their resources at a more local level. Reducing backhaul requirements, by far the most expensive component of LTE networks, in turn decreases operational expenditures. Additional capabilities of decentralized networks will be enabled by technologies such as mini-mesh networks, increased use of deployables and small cell eNodeB's, and leveraging Internet of Things (IoT) technologies such as Wi-Fi, Bluetooth and cellular 5G. 3GPP began to address these capabilities in LTE Release 10 with improvements on performance at cell edges,[59] and has continued in Release 12 with the self-configuration of enhanced small cells and new and enhanced services of device-to-device communications.[60] Moving forward, the Analytics Working Group anticipates that public safety will benefit from a decentralization of functions like analytics, where analytics are performed at the edge, conserving critical network bandwidth for other traffic and functions.

Enabled Operational Capabilities: Improved Situational Awareness, Improved Information Management and Data Triage, and Improved Network Analytics

The Analytics working group identified Improved Situational Awareness, Improved Information Management and Data Triage, and Improved Network Analytics as critical operational objectives of future R&D to support the public safety community. Specific to analytics, the main technology capabilities that arise from R&D directed at these enabled operational capabilities include:

Technology Capabilities, Gaps, and Barriers

The Analytics Working Group identified several key technology gaps that need to be addressed before analytics run across decentralized networks can become a reality for public safety. These gaps and the technology capabilities with which they are associated are listed in Table 8 below.

[59] http://www.sonlte.com/lte-roadmap/

[60] http://www.unwiredinsight.com/2014/highlights-of-3gpp-release-12

1. Connecting user devices to serve as their own mini-mesh networks

Wireless local area networks (WLANs) rely on a traditional, “hub and spoke” model to provide Internet access to user devices. In this model, each device must connect to a centralized point in order to access the Internet. Conversely, mini-mesh networks, or wireless mesh networks (WMNs) use multi-hop connectivity to send and receive data, meaning users are connected to each other instead of being directly connected (single hop) to the wireless router.[61] Mesh networks can also boost signal or find a shorter route to fiber than current centralized network architectures. As public safety continues to operate in a multi-network environment (LMR, commercial broadband, and eventually the FirstNet network), mini-mesh networks may provide a critical capability for public safety operations. To the extent that decentralized networking solutions can expand the functionality of and enhance access to public safety communications during this moment of transition to next-generation technologies, WMNs and mobile ad hoc networks may be one aspect of a more diversified approach.[62]

Gaps & Barriers
Currently device technology vs. network technology is divided. This would require a paradigm shift and consideration of modularized components that serve multiple purposes.

2. Analytics will move to the edge of the network to reduce network congestion

One aspect of the network decentralization trend is the movement of functions and capabilities from the network core to the network edge, including analytics. This is especially important for Video Analytics, which cannot be transmitted across and LTE network at scale. Recent improvements in the design and processing power of Digital Signal Processor (DSP) chipsets have made it possible for Video Analytics software to operate highly effectively for some use cases at the edge. This offers a major benefit to IP network-based surveillance systems in that HD cameras can be deployed without excessive network bandwidth utilization.[63] The Analytics Working Group stated the importance of pushing as much analytics to the data creation point (edge) as possible to reduce strain on the network. Analytics at the edge will also enable the integration of IoT technologies into public safety operations. Technologies such as cellular 5G and Bluetooth will eventually enable data created by IoT and multiple sensor devices to better support public safety decision-making.

Gaps & Barriers
Need for market analysis to determine total addressable market to drive industry R&D investment.
Data processing power of the analytic.
If you move analytics to the edge, you will enable devices to interact at the edge of the network as well. Some devices will push data, some will request data, which means that analytics will need to support this “up and down” processing. Need to design architecture to support this.

[61] https://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Public_Networks_for%20Public_Safety%20Briefing_Document.pdf
[62] https://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Public_Networks_for%20Public_Safety%20Briefing_Document.pdf
[63] http://www.vcatechnology.com/news/articles/video-analytics-on-the-edge/

3. Deployables and small cell eNodeB will be increasingly required and prevalent over time

As public safety transitions to LTE technology, the role of deployables and small cell eNodeB's will become increasingly important. Public safety is currently gathering lessons learned through the JerseyNet project in the State of New Jersey. "JerseyNet is designed to include more than 30 cells on wheels (COWs) and six systems on wheels (SOWs) that can be deployed in various locations via SUVs, vans or trailers"[64] Deployable assets such as these will provide additional coverage and capacity during emergency response. When partnered with 'analytics at the edge' as discussed previously, public safety will be able to bring powerful analytical tools to the scene of incidents, regardless of topography or fixed infrastructure. Another key aspect of deployables identified by the Analytics Working Group was cybersecurity. Analytics could improve cybersecurity and encryption of these new networks that will become the target of malicious threats. As discussed in the 2012 NPSTC High Level Broadband Launch Requirements: "The NPSBN SHALL have a set of tools for analyzing and monitoring system and user data to determine possible threats to the network before they occur or to support post-event activities."[65]

Gaps & Barriers
The SWaP of deployable technologies has only recently become acceptable for testing and initial operational integration with public safety nationwide.
Cognitive barrier to the shift from a fixed tower first with limited deployable architecture to an architecture where deployables are more prevalent.
Integration of LTE-U and other technologies to improve coverage and resiliency with public safety networks without disrupting other networks.
Security modeling development.
Automatic detection of cybersecurity threats including man-in-the-middle detection.

[64] http://urgentcomm.com/public-safety-broadbandfirstnet/vendor-team-outlines-features-all-deployable-public-safety-lte-netwo

[65] http://www.npstc.org/download.jsp?tableId=37&column=217&id=2609&file=BBWG_SoR_Launch_12112012.pdf

Enabling Actions & Actors

What's being done? Who's doing it? How will remaining gaps and barriers be addressed?

This section is not intended to be an exhaustive review of all enabling actions and actors currently working on decentralization of networks related analytics efforts. Rather, it is intended to provide a brief sample of R&D efforts both inside and outside of the pubic safety sector that represent the partnerships that public safety R&D organizations could build. Continued market research will be necessary to create awareness of current efforts and account for new actors in these fields.

Mesh Networks

- Firetide/Houston, TX Police Department – "Using a Urban Areas Security Initiative (UASI) grant from the U.S. Department of Homeland Security, Houston Police deployed Firetide's HotPort Wireless Mesh network to enable high-definition video surveillance of 134 downtown intersections. Firetide's multiple input, multiple output (MIMO) wireless mesh network includes built-in redundancy, as the mesh will always send the traffic down the best available path. If one node should happen to go down…,the traffic automatically reroutes to the next best available path. The wireless mesh network connects to the city's existing fiber network at four backhaul points. This self-healing capability helps minimize downtime, since there are multiple routes back for every node on the network."[66]
- HP – "is working on the movement of data between cars networked together, rather than each car being connected into a central system or cloud. It envisages that cars, or nodes in other networks of things, will have their own processing and storage capabilities so that they can 'talk' to one another rather than necessarily with a central network."[67]

Deployables/Small-Cell eNodeBs

- Oceus – "Oceus Networks provides a…System on Wheels (SoW) based architecture. This type of solution pushes the network cores and application services out to the edge of the network to make each cellular node a self-sufficient system."[68]
- General Dynamics Mission Systems – "Partnering with Texas A&M University, Texas National Guard, Texas Task Force 1, and other Texas public safety agencies, along with the EDGE Innovation Network and members, General Dynamics Mission Systems successfully demonstrated its Band Class 14, 4G LTE network at the EDGE Innovation Network's 2013 Winter Institute held at Texas A&M University's Disaster City training facility using the Cell-on-Wheels (COW)."[69]

Analytics at the Edge

- IBM – "announced in March 2015 that it would invest $3 billion over the next four years to establish an IoT unit.**"[70]**

[66] https://www.firetide.com/files/9614/0122/6089/Houston_FiretideCaseStudy-web.pdf
[67] https://451research.com/report-short?entityId=87166&referrer=marketing
[68] http://www.oceusnetworks.com/public-safety/
[69] http://gdc4spublicsafety.com/our-deployable-solution/
[70] https://451research.com/report-short?entityId=87166&referrer=marketing

- Cisco – "in 2015 acquired ParStream which had developed a database platform for use primarily in IoT applications with the ability to run R or Python to perform analytics at the edge."[71]
- Intel – "has established two IoT labs, one in Santa Clara, California, and another in Limerick, Ireland to allow customers to test and deploy IoT solutions and devices with the ability to demonstrate large workloads, connectivity, and data modeling and extraction."[72]

Public Safety R&D Opportunities

What project ideas should Public Safety R&D organizations consider as they prioritize upcoming investment opportunities?

Given the technology capabilities, gaps and barriers, and enabling action and actors that are forecasted to impact the analytics domain over the next 20 years, the Analytics Working Group identified several potential R&D efforts that would enable more effective analytics for public safety based on the decentralization of networks. Public Safety R&D organizations should consider the following project ideas as they prioritize upcoming investment opportunities:

- Explore dynamic spectrum allocation and software-defined radios for public safety use
- Explore constructive interference R&D to maximize spectrum usage and limit harmful interference
- Explore potential of low cost (<$1,000) and low SWaP communication technologies
- Encourage development of capabilities relevant to public safety in open source projects (i.e. OpenWRT, DD-WRT, etc.)
- Conduct an evaluation of Prose and SON technologies
- Research/define how deployables and small cells would improve or hinder operations in regards to data analytics support
- Conduct a network edge trade study to include industry (equipment manufacturers, start ups, and carriers), academia, and federal partners
- Identify common data requirements across analytics, so we can prioritize data for analytics
- Investigate modularization of network components that serve multiple purposes for the use of creating resilient mesh networks
- Design an architecture to support the 'up and down' processing of analytics at the information edge

[71] https://451research.com/report-short?entityId=87166&referrer=marketing
[72] https://451research.com/report-short?entityId=87166&referrer=marketing

Conclusion

This initial Public Safety Analytics R&D Roadmap generated a great deal of input, ideas, and opportunities for PSCR and other R&D-focused agencies, industry, and academia to consider. The potential impact on the public safety community can be tremendous given the appropriate and successful application of R&D funds to address some of the opportunities listed in this report. PSCR intends to continue to build upon the Public Safety Analytics R&D Roadmap as it identifies, vets, and plans R&D projects. Meanwhile, PSCR will launch additional roadmapping efforts to identify similar opportunities for technology advancement in the interest of equipping the public safety community with the most effective technologies possible to save lives and property.

PSCR would again like to thank those who contributed to the completion of this roadmap, those who attended the June 2015 PSCR Stakeholder Conference in San Diego, California, and particularly those who were members of the PSCR Public Safety Analytics Working Group listed in Appendix A.

For more information on PSCR and its programs, please visit www.pscr.gov.

Appendix A: Public Safety Analytics Working Group Members

Name	Company/Agency
Alex Hauptmann	Carnegie Mellon
Andy Thiessen	PSCR
Andrew Weinert	Massachusetts Institute of Technology Lincoln Laboratory
Barry Luke	NPSTC
Barry Leitch	FirstNet
Benjamin Posthuma	Northrop Grumman
Bill Schrier	Seattle, WA Police Dept.
Bruce Cox	NextNav
Chief Mike Duyck	Tualatin Valley, OR Fire & Rescue
Chris Gates	NextNav
Chris McIntosh	ESRI
Christian Militeau	Intrado
David Debrecht	Nokia
David Jenkins	IBM
David McCarron	TilsonTech
Denise Masi	Noblis
Dharmesh Tyagi	Nokia
Diamond Chaflawee	NICE
Don Dejewski	IBM
Don Bradshaw	PSCR
Ed Mills	Colorado OIT
Elizabeth Gray	Austin, TX Fire Dept.
Farook Hussan	Samsung
Gary Monetti	Monetti & Associates
Gary Nestler	IBM
Geoff Spring	Melbourne University, Australia
Greg Bazick	Ann Arbor, MI Police Dept.
Lea Ann Hart-Chambers	Oregon Dept. of Transportation
Hong Kim	IBM
Jason Schiess	Durham, NC Police Dept.
Jeff Posner	FirstNet
Jennifer Hansen	LR Kimball
Jeremy Benson	NIST
John Aviles	IBM
John Contestibile	Johns Hopkins Applied Physics Laboratory
John Garrafolo	NIST
John Lenihan	LA County, CA Fire Dept.
Joe Heaps	US Dept. of Justice
Karen Allen	AZ DOA
Ken Baker	Colorado University
Kevin Gifford	D.C.S Gifford LLC
Kim Coleman-Madsen	Colorado OIT

Name	Company/Agency
Lisa Sokol	IBM
Mark Golaszewski	FirstNet
Mark Jones	NOBLIS
Mark Adams	NGC
Mike King	ESRI
Natalie Baker	Intrado
Neal Fishman	IBM
Nelson Hastings	NIST
Patrik Ringqvist	Ericsson
Prince Niyyar	Commdex

Name	Company/Agency
Peter Williams	IBM
Gina Harrison	NTIA
Robert Green	IBM
Robert Escalle	Sonim Tech
Steve Kropper	Parallel Wireless
Terri Brooks	Sierra Cedar
Tracy McElvaney	PSCR
Wilbur Smith	Brocade
Walt Magnussen	Texas A&M University