HIGHLY MOBILE DEPLOYED NETWORKS

PSCR Highly Mobile Deployable Networks R&D Summit Report

U.S. DEPARTMENT OF HOMELAND SECURITY

CTL Communications Technology Laboratory

NIST

PSCR

Sponsorship

The Highly Mobile Deployed Networks project is sponsored by the Department of Homeland Security (DHS) Science and Technology (S&T) Directorate. The project is managed by the DHS Next Generation First Responder Apex Program and the Public Safety Communications Research (PSCR) DHS portfolio within the National Institute of Standards and Technology (NIST) Communications Technology Laboratory (CTL). It is complementary research to the PSCR Resilient Systems Research and Development (R&D) efforts.

Deployable systems (DS) are a critical component for providing coverage to Next Generation First Responders (NGFR) under the Nationwide Public Safety Broadband Network (NPSBN). Availability of DS is expected to be a critical need for remote areas where complete coverage is not feasible, areas with extreme congestion due to large-scale events or incidents, and areas where installed resources are compromised. Under this project, PSCR is conducting research into DS interconnectivity to create a sophisticated network to allow for enhanced interoperability in incident areas.

Table of Contents

Purpose of the Summit

The Public Safety Communications Research Program (PSCR) convened over 85 stakeholders at the Department of Commerce Boulder, CO campus to discuss the opportunities and challenges facing public safety's expanded use of next-generation deployable systems. This two-day event took place October 18-19 and provided stakeholders an opportunity to provide input on public safety's requirements and desired outcomes for the "Next Generation Deployable Network," defined by PSCR as multiple independent LTE networks operating in conjunction with one another to augment the existing public safety broadband network. Summit attendees brainstormed how to advance LTE architecture, resiliency, backhaul, and other potential solutions more effectively to support two high-priority deployable network use cases which were identified by PSCR:

- Dynamic Incident Area Network with No Existing Coverage or Backhaul
- Dynamic Coverage of Existing Network, Intermittent Backhaul

On day 1 of the Summit, stakeholders brainstormed specific technology and knowledge gaps inhibiting the expanded use of deployable systems in both of these use cases. These gaps were then used to brainstorm possible deployable network solutions on Day 2.

The Summit concluded with a plenary brainstorm session on what represents the critical elements of a Deployable Networks Test Bed, what technologies could be evaluated in this test bed, measurement approaches and experiment designs to evaluate the effectiveness of these technologies, key performance indicators, and challenges to consider when testing identified technologies.

Following the Summit, PSCR hosted a deployable network capability demonstration at the Table Mountain Field Site located about 20 minutes north of Boulder. The demonstration featured two self-contained LTE networks with independent application servers, users, and mesh network architecture. This exercise demonstrated the highly mobile deployed network concept where multiple individual LTE-based incident area networks can converge to share applications, information, and users. The details of this demonstration are captured in the "Field Demonstration Report" which was released as a deliverable to DHS on October 30th, 2017.

The meeting agenda for the Summit is provided below:

Day 1 (Wednesday, October 18)

9:00am	Opening, Introductions, FirstNet Keynote Address
9:30am	Identifying Gaps for Use Case 1 - Dynamic IncidentArea Network with No Existing Coverage or Backhaul (Breakout #1)
1:30pm	Use Case 1 Gaps Brainstorm Report Out
2:00pm	Identifying Gaps for Use Case 2 - Dynamic Coverage of Existing Network, Intermittent Backhaul (Breakout #2)
3:45pm	Use Case 2 Gaps Brainstorm Report Out
4:30pm	Day 1 Closeout

Day 2 (Thursday, October 19)

9:00am	Day 1 Recap
9:15am	Developing Solutions for Use Case Gaps (Breakout #3)
11:30am	End-to-End Solutions Report Out and Discussion
1:30pm	Providing Value to Public Safety Through a Common Deployables Test Environment (Plenary Session Q&A)
2:30pm	Designing Experiments and Measurement Approaches for Deployables Test Environments
4:00pm	Summit Hotwash & Closeout

Gap Themes Affecting Next Generation Deployable Systems

The Summit resulted in a list of four fundamental deployable network technology gap areas that align with public safety needs and requirements. These four focus areas will help inform the development of potential R&D project opportunities for research organizations supporting public safety technology to consider going forward. These gap themes include:

1. **Machine Learning** - The self-optimization of a computer process through iteration. This theme will focus on machine learning to have the network self-optimize decision-making and network efficiency.
2. **Open Interfaces** - The development of a standard input and output relationship between equivalent systems. Networks should be able to communicate through common interfaces and processes for cooperation and communication over the air.
3. **Dynamic Access** - The ability for systems and devices to get access to the resources and data that they need. The focus of this theme is how the system determines who can access data, where it is accessed, and how it is accessed. This topic expands to cooperation between networks to serve users on the ground.

4. **Deployable Characterization** - Different deployables are needed for different types of situations and agencies. This theme represents the documentation and categorization of deployable systems.

Participants brainstormed many specific gaps that align to one of the four themes described above. Some of the specific technology gaps that are within scope for PSCR research consideration include:

1. Machine Learning
    i. The inability for automatic intelligent decision-making for data routing, storage, and processing.
    ii. The inability for a network to self-organize for greater coverage and resource distribution.
2. Open Interfaces
    i. The inability for deployables from different vendors to recognize and cooperate with each other.
    ii. The need for new data protocols specific to the operation of deployable systems.
    iii. Common interfaces between network information and user applications do not currently exist.
    iv. No defined standard for decentralized core-to-core communication.
3. Dynamic Access
    i. Inability of deployed networks to gather information about neighboring networks and other systems and parameters within the ecosystem.
    ii. No ad hoc roaming agreement ability.
    iii. No global offline authentication solution and no easy method for the addition of new users.
    iv. No data integrity and security implementation when an operation is over.
4. Deployable Characterization
    i. Deployable capabilities are not organized for operational use and are not optimized to an agency's operational needs.
    ii. No information or in-depth description of the deployed network architecture.

In addition to the themes described above, Summit participants identified several technology gaps that represent interesting opportunities for deployable system research organizations. The following data is not meant to serve as an exhaustive accounting of every technical issue discussed. Rather, this report intends to characterize the highlights from input collected at the Summit with sufficient technical detail.

Deployables R&D Theme #1 -- Machine Learning

PSCR has defined the Machine Learning theme as it relates to Deployable System R&D as "the self-optimization of a computer process through iteration. This theme will focus on machine learning to have the network self-optimize decision-making and network efficiency."

Within this theme, participants focused on characterizing the challenges for enabling deployable networks to improve analytics-supported decision-making for network optimization, and to self-organize for optimal coverage. Participants brainstormed specific problem statements and potential end-to-end solutions within each gap area. Highlights from these discussions are provided below:

Gap 1.1 -- The inability for automatic intelligent decision-making for data routing, storage, and processing

Problem Statements:

Deployable Systems (DS) need to have decision making algorithms to determine what processes to do where and at what time. For example, if a backhaul connection is available, but not sufficiently reliable, the system should be able to decide what applications or users get priority on this small "pipe". The system should also be able to decide which application server, local or within the cloud, it should use when given a user request. QoS considerations and local network resource scarcity/availability would inform the DS on what these decisions should be. This process would also be applied to overall network management to optimize other DS on the network. This means that the DS knows about the resources capabilities, connection quality, and availability of other systems on the local network. Making routing and application processing decision with the knowledge of other systems in the network would drastically improve the network's capabilities as a whole and reduce network congestion.

The system should also know when and where it should replicate database information. This is necessary in a deployable scenario because the network can be easily fragmented and disconnected from other DS. Adding redundancies within the network leads to continued service to users even if network connections are broken. This will also lead to the reduction of internetwork traffic. As well as adding redundancies in the network, these decision-making algorithms would also aid in data synchronization decisions. This means that the algorithm can handle what to do with duplicate data within the network.

Potential End-to-End Solutions:

1. The implementation of machine learning to improve load balancing and bandwidth management for Centralized Self-

Optimizing Network (CSON) and Decentralized Self-Optimizing Network (DSON). This solution requires that the DS needs to formulate a predictive model given all the information available about the network. From this model, consequences of different network configurations can be made available to the system.

2. Store data with timestamps to allow for data synchronization. If we have multiple pieces of data of the same thing (i.e. first responder location information) then the hierarchy of whose data is correct is determined by the timestamp. Further metadata could be implemented when collecting information in the field to inform a DS about what the piece of information is or could contain. This metadata would allow for User Equipment (UE), a DS, and the greater Public Safety Broadband Network (PSBN) to synchronize data.
3. Extending cloud replication to an intermittent connection or island connection for service resiliency. This would be the replication of important data that needs to be on site at all times to multiple locations/nodes on the network. This requires a replicated copy to be on different DS so UE can always have access to it.
4. At the application level, applications must feature QoS / bandwidth management mechanism to decide what to store, purge, and prioritize when a connection is established. This is different then the network level machine learning as the application must be able to make these decisions as well. With both the network and the application working together on processing necessary/relevant data, overall network traffic will be lowered.

Gap 1.2 -- The inability for a network to self-organize for greater coverage and resource distribution

Problem Statements:

Deployable networks, due to the lack of resources available to them, must be able to self-organize the systems that are available to provide an incident area with the best possible coverage and resource distribution. Currently this management is manual and requires a dedicated network manager. This process needs to be automated and integrated into the network.

DS need to understand their own RF environment and determine their own placement as well as the placement of other networks to optimize coverage over an incident area. An example of this self-organization is that if a system detects that it is interfering with another system, then both systems need to adapt and adjust to reduce the interference. Not only should the DS make these decisions on scene, but some pre-deployment recommendations should be made to optimize the network before responders arrive.

Resource distribution applies to network coverage as well as traffic prioritization. DS need to implement some way of routing traffic within a network to optimize service to its users. Traffic priority based on content, data type, and user hierarchy need to be parts of a DS decision-making matrix. Further, if too much traffic is trying to be pushed in the network, DS need to have responses to try and reduce this congestion the best they can. This could be the use of different servers or connections within the network.

Potential End-to-End Solutions:

1. Dynamic SONs have been an implementation in 3GPP for the planning, configuration, management and optimization of a RAN. An intelligent SON built for the deployable architecture can solve many of the resource distribution problems that currently face the multi deployment scenario. RAN self-healing, and graceful degradation would be key in SON functionality.
2. Highly intelligent resource mapping before and during deployment would solve many organizational problems. A decision-making algorithm could be implemented to provide recommendations of placement locations of where a DS should be in an incident area. This algorithm would leverage information based on previously known factors about an area (geography, incident area location, incident type, possible existing coverage, etc.) as well as its own capabilities. During deployment the DS can self-analyze the network to update the incidents resource map and make changes to the network.
3. Enhanced system analytics to optimize services with predictable user experience. This goes beyond deployable placement and into application server and database locations within a network. If multiple users start to use a particular service, a deployed network needs to know to turn on application servers to fulfill the demand of the network. On the other hand, DS should be able to turn off services to save power when not in use.
4. Create an end-to-end path assessment for UE. This would be the analysis of all the available paths that data can be pushed through followed by the decision, based on network conditions, to choose one of the paths. This solution may include a mesh network link between networks in an operational area, but goes further in having the DS make some of those routing decisions as well as the mesh system.

Deployables R&D Theme #2 -- Open Interfaces

PSCR has defined the Open Interfaces theme as it relates to Deployable System R&D as "the development of a standard input and output relationship between equivalent systems. Networks should be able to communicate through common interfaces and processes for cooperation and communication over the air."

Within this theme, participants focused on characterizing the challenges related to how deployables can recognize and cooperate with each other through new protocols, interfaces, and network architectures. Participants brainstormed specific problem statements and potential end-to-end solutions within each gap area. Highlights from these discussions are provided below:

Gap 2.1 -- The inability for deployables from different vendors to recognize and cooperate with each other

Problem Statements:

In the multiple highly mobile deployment scenario, public safety will have multiple networks within an operational area with their own coverage area serving their own home users. These systems currently do not have a way to communicate with one another automatically or to coordinate overall communication management. This network-to-network setup needs to be in operation as soon as first responders arrive on scene, which must be carried out with little to no user input needed.

Communications between DS need to be robust and maintain connections when conditions change. Network-to-network connections need to be self-healing and mobility tolerant as with a mesh network topology. The primary technology gap that we have identified is that the mesh subsystems in DS must be able to communicate with each other, over the air, regardless of their mesh protocols.

Potential End-to-End Solutions:

1. Establishment of an over the air standard interface for mesh nodes from different vendors to communicate. This means that mesh radios, despite having their own proprietary waveform, could also contain some sort of general waveform that can communicate with other mesh radios in an incident area.

Gap 2.2 -- The need for new data protocols specific to the operation of deployable systems

Problem Statements:

Many different internet protocols (IP) break down in the highly mobile deployed network due to the nature of the network. UDP/TCP/ SIP protocols cannot manage the congested and constantly broken network. Deployable systems need new network protocols mainly for hybrid routing, power efficient network discovery, and disruption-tolerant networking. These protocols need to deliver the same quality of service as would normally be provided in a fixed network.

Potential End-to-End Solutions:

1. Disruption Tolerant Networking for Public Safety. DTN can replace common IP protocols and eliminate duplicate data allowing for less congestion and greater optimization of the deployable network.

Gap 2.3 -- Common interfaces between network information and user applications do not currently exist

Problem Statements:

This can be summarized as two sub technology gaps. The first being that application developers need to get information about the health/status of a network to optimize the performance of their applications. Within the deployables space the network topology is vastly different than in the fixed network and can lead to degradation of an application's performance and even breakdown of the application. Application developers need to get live information about what the network is so they can allow the application to pivot under network strain.

Secondly, network information needs to be disseminated to end users. Users need to know what is happening to the network and the available capabilities in real time.

The DS needs to let both users and applications know if there is significant network congestion and if the user's communications are going to get through. For example, if the network is only allowing emergency type data though, then the network needs to inform

applications and users. The DS also needs to inform users and applications if there is a backhaul connection and its configuration. As well as connection types, the DS needs to give information about who and what can be reached within the network.

Potential End-to-End Solutions:

1. Common services such as Application Programming Interface (API) and Service Provider Interface (SPI) for network to application communication needs to be implemented and standardized for deployable systems. A follow up evaluation on current application standards to implement this network health API/SPI needs to be considered.
2. The development of a standardized iconology or network notification system to UE that informs users of their capabilities within the network. Network health and capabilities would be disseminated through this notification system.

Gap 2.4 -- No defined standard for decentralized core-to-core communication

Problem Statements:

LTE cores currently cannot communicate with each other in an automatic and decentralized way for RAN management, data synchronization, and user roaming. This technology gap leads to the inability for DS to synchronize with each other as well as properly coordinate. Information that core networks may need to share include PCRF rules and HSS subscriber information. Ad hoc core information sharing with another core is a technology that does not exist within the 3GPP standard.

Potential End-to-End Solutions:

1. The development of a protocol to have EPCs automatically discover one another when network connections are established.
2. The development of InterCore communication protocols that utilize the S10 interface. This communication is expected to be made through a mesh connection between each core.

Deployables R&D Theme #3 -- Dynamic Access

PSCR has defined the Open Interfaces theme as it relates to Deployable System R&D as "The ability for systems and devices to get access to the resources and data that they need. The focus of this theme is how the system handles who gets what, where they get it, and what the best way to get it. This further expands to how networks cooperate to serve users on the ground."

Within this theme participants focused on characterizing the challenges related to ad hoc roaming, user identification and authentication, and data management. Participants brainstormed specific problem statements and potential end-to-end solutions within each gap area. Highlights from these discussions are provided below:

Gap 3.1 -- Inability of deployed networks to gather information about neighboring networks and other systems and parameters within the ecosystem

Problem Statements:

There is a lack of tools and standards to measure, model, and predict network coverage, capabilities, load, and connection reliability before and during DS operations. DS needs to inform users and applications about what the system may be able to provide in terms of coverage, information, quality of network connections, and analytical tools before the system arrives on scene. This information would come from the DS own capability set.

Along with prior analytics, DS should be able to measure and analyze, in real time, the environment and network to inform users and applications of the coverage, application capabilities, availability, and quality of network connections. The network should be able to measure if there is significant interference in the area, what its own coverage area may be, its connection quality to other deployables in the area, and what kind of backhaul connection the network may have.

Potential End-to-End Solutions:

1. Utilize existing industry diagnostic applications.
2. Construct a framework for capturing sufficient information to analyze a network.
3. Develop a predictive model of configuration overhead and consequences that may be used with machine learning techniques to make routing and processing decisions.
4. Develop an always-on, low overhead, and intelligent RF sensing algorithm for coverage and interference

measurements.

5. Develop an always on, low overhead, and intelligent network load reporting system.
6. Break out MME information to divulge information about who is on the network.

Gap 3.2 -- No ad hoc roaming agreement ability

Problem Statements:

There is currently no automatic method coordinating a roaming agreement between two networks. Specifically, when two or more LTE networks exist in a common operational area, no protocol exists that can automatically set up a roaming agreement. A decentralized process is needed for forming and managing the new larger network. User authentication, MME-MME coordination, and other network core responsibilities need to be managed for roaming to be available. Traditionally, roaming agreements between networks is a preplanned technology and relies on a fixed network architecture. In the highly mobile scenario, these agreements need to be made right away once deployables are able discover each other.

DS need to establish ad hoc roaming agreements so that users can operate anywhere within the larger local network. This roaming agreement should be automatic with no manual input required from users. Further, data sessions with users must be maintained so that there is a smooth transition from one network to another. This capability is known as session persistence, and it means that at the application layer, as well as at the network layer, applications will continue their connections to other nodes in the network.

Potential End-to-End Solutions:

1. Look toward standards that have already been implemented in 3GPP to solve this issue for the HMDN case: solutions involving coordination between EPCs for MME handoffs and HSS database synchronization. The next step would be the modification and implementation of these standards for the automatic and decentralized criteria. A decentralized coordination between EPCs could involve deciding which EPCs to “turn off” and which EPC should assume control of the deployed network (orchestration). This feature will become standardized in 3GPP release 15.
2. There is a need to create standards for session persistence that deals with a changing IP address when roaming between networks.
3. The ad hoc roaming problem could also be solved by Customer Owned and Maintained (COAM) synchronization with the FirstNet Core. This solution would lead to dynamic node or core configuration when multiple systems are brought on scene.

Gap 3.3 -- No global offline authentication solution and no easy method for the addition of new users

Problem Statements:

When a deployable network is disconnected from the macro network, or PSBN, users still need to be authenticated on the deployed network as they come on scene. A backhaul connection to connect to an authenticating core is not always guaranteed in an incident area, so there is a need for an offline authentication system.

Even with a general offline ICAM solution, there is no easy way to enter new users into the system. Ad hoc HSS entry requires network management knowledge and manual configuration, which not only wastes time and effort but also detracts from the primary focus of first responders. A new way for ad hoc authentication is required for a secure and fast way to enter users onto the system.

Potential End-to-End Solutions:

1. An offline Identity, Credentials and Management (ICAM) system is currently under development.
2. Role Based Identification. The current authentication system cannot send entire credentials up the chain, so a system could be implemented where the credential database is replicated to other nodes in the network. Define the process that identifies users/devices and provides them with appropriate security clearance
3. Usage of SmartSIMs for first responder equipment. SmartSIMs allow users to re-key their identity. Review whether these can be deployed in a viable way in the case of a large-scale emergency
4. Review the current LMR Authentication Process for practices that may be applied to LTE networks. For example, LMR radios have IDs that are affiliated with a network.

Gap 3.4 -- No data integrity and security implementation when an operation is over

Problem Statements:

With a multiple deployment scenario where user databases and agency information are being routed through various systems and shared on multiple networks, there arises a problem of cross data contamination and a potential breach in agency data security. For example, if one deployable shares HSS information with another to allow for user authentication on a different core, then that data is now located off the home agency's network and in a potentially vulnerable place. No mechanism exists to control this dissemination of data in a secure way.

Potential End-to-End Solutions:

1. Create a technology to manage data retention/expiration. Develop a schedule dictating which public records need to be retained to adhere to policies.

Deployables R&D Theme #4 -- Deployable Characterization

PSCR defined the Deployable Characterization theme as "representing the documentation of deployable systems and the outline of different types of deployables that could be available to first responders."

Within this theme, participants focused on characterizing the challenges related to optimizing deployable hardware for operational use. Participants brainstormed specific problem statements and potential end-to-end solutions within each gap area. Highlights from these discussions are provided below:

Gap 4.1 -- Deployable capabilities are not organized for operational use and are not optimized to an agency's operational needs

Problem Statements:

There is a need to optimize size, weight, and power of deployable hardware for different tasks, agencies, and environments and classify these optimizations. Deployable systems can be built from many different components and subsystems that not all agencies need or can have. The addition of functionality may lead to the restriction of mobility and endurance for the deployable that are not needed by, or available to, all agencies. Minimum requirements need to be specified for a deployable system for general scenarios.

Further, it is important to develop a categorization of deployable systems so agencies know what functionality comes with what deployable. For example, a DS classified as a class 1 deployable would only bring LTE coverage, but no application server, where as a class 2 deployable could have LTE coverage and an application server.

Potential End-to-End Solutions:

1. Develop a categorized list of general systems for different levels of deployables. This list would include detailed estimates about the endurance, weight, dimensions, and capabilities of the deployable.
2. Develop a high-level optimization scheme to provide to vendors and first responder groups general guidelines of what might be needed for general use cases.

Gap 4.2 -- No information or in-depth description of the deployed network architecture

Problem Statements:

Detailed description of the deployable network architecture is currently not standardized or known in general. Beyond theoretical predictions for the deployed network, no designed experiments have been conducted on how the network will operate. Application and hardware developers do not have data or requirements to allow tailoring their products to the deployable network, and thus their products may not be optimized or even compatible with the network.

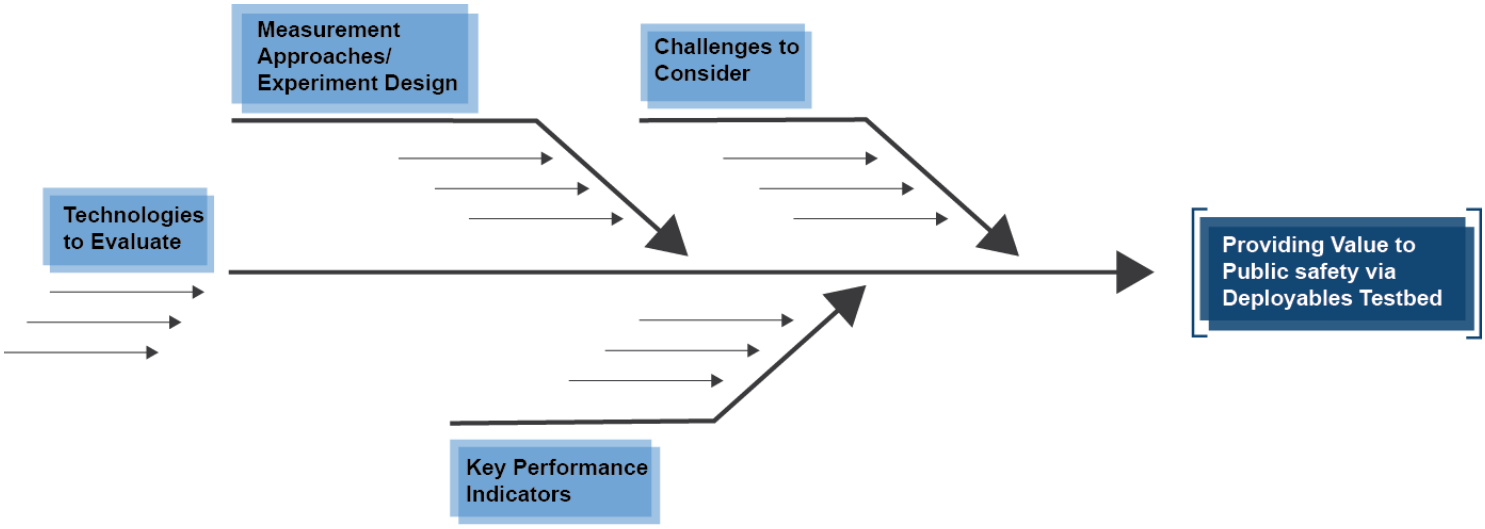
Potential End-to-End Solutions:

1. Develop a very specific outline of the future state of deployable system. The document would be intended to target application developers in order to inform them of how the network should perform, react, and change over time.
2. Field tests and trials of this network architecture must be performed to get data concerning how the system works in a live scenario. The architecture needs to be researched and measured in a real environment to fully describe the network.

Providing Value to Public Safety through a Deployables Test Bed

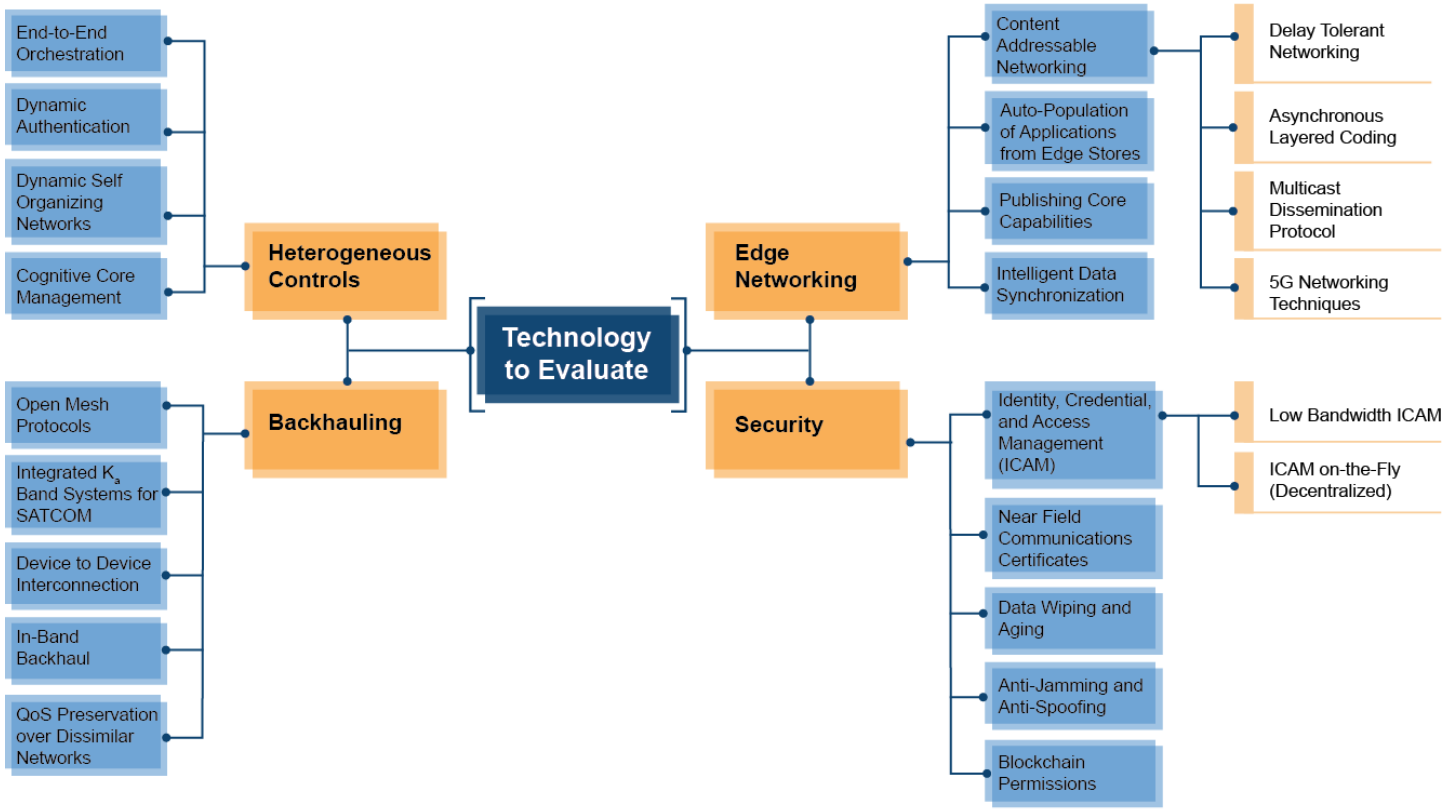
After characterizing technology gaps affecting deployable networks research topics, participants were asked to evaluate the ways in which a deployable networks test bed could provide value to public safety and the associated research communities. Attendees were invited to brainstorm specific requirements for potential test beds, capabilities to evaluate in testing environments, and potential challenges to consider. Participants provided input aligning with four attributes of a deployable networks test environment: 1) Technologies to Evaluate, 2) Measurement Approaches / Experiment Design, 3) Key Performance Indicators, and 4) Challenges to Consider.

The exercise was intended to mirror the workflow associated with establishing a network testing environment. To that end, attendees were first asked to identify the technologies to bring to the test bed and describe ways in which one could evaluate the effectiveness of deployable solutions within this environment. The group then pivoted to identify relevant metrics that would indicate progress and challenges that deployable researchers should consider when measuring the impact of these technologies. The graphic below illustrates the logic behind this breakout exercise:

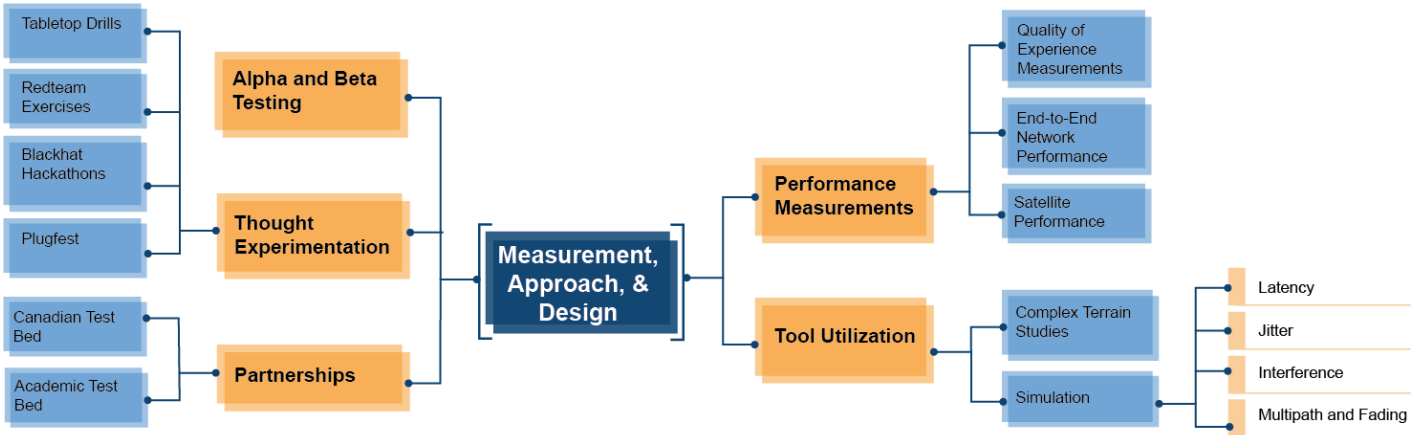


The graphics below highlight the themes that resulted from participant brainstorming within each component of a potential deployable networks test environment:

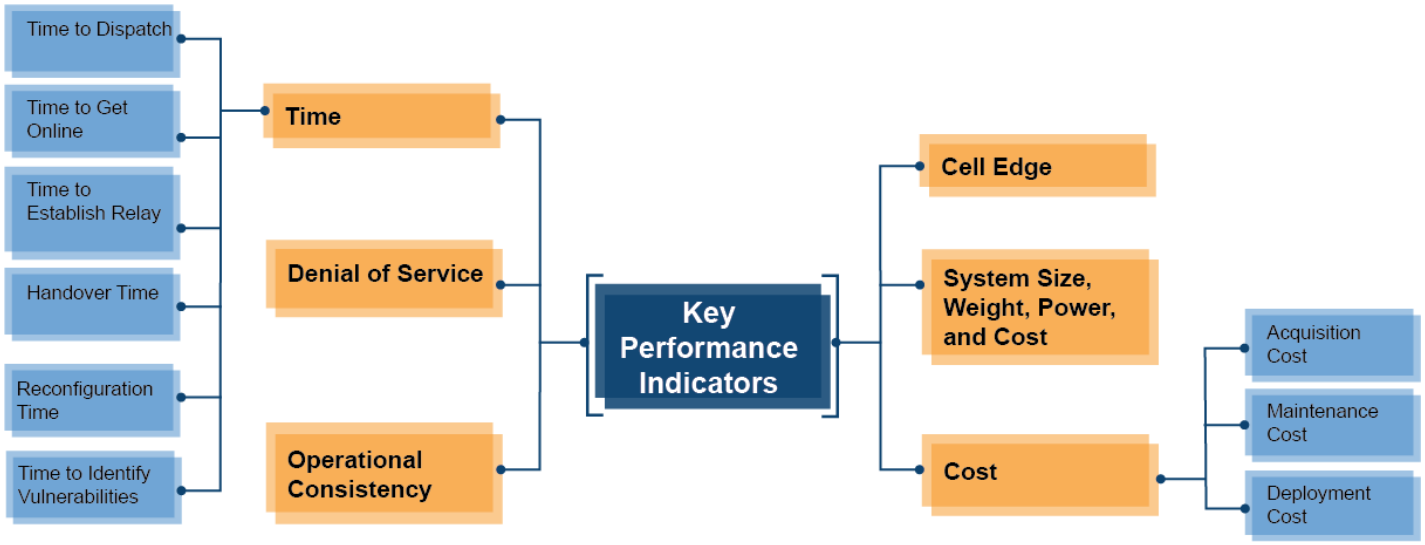
Technologies to Evaluate -- *What existing or forthcoming deployable solutions could be brought to a testing environment?*



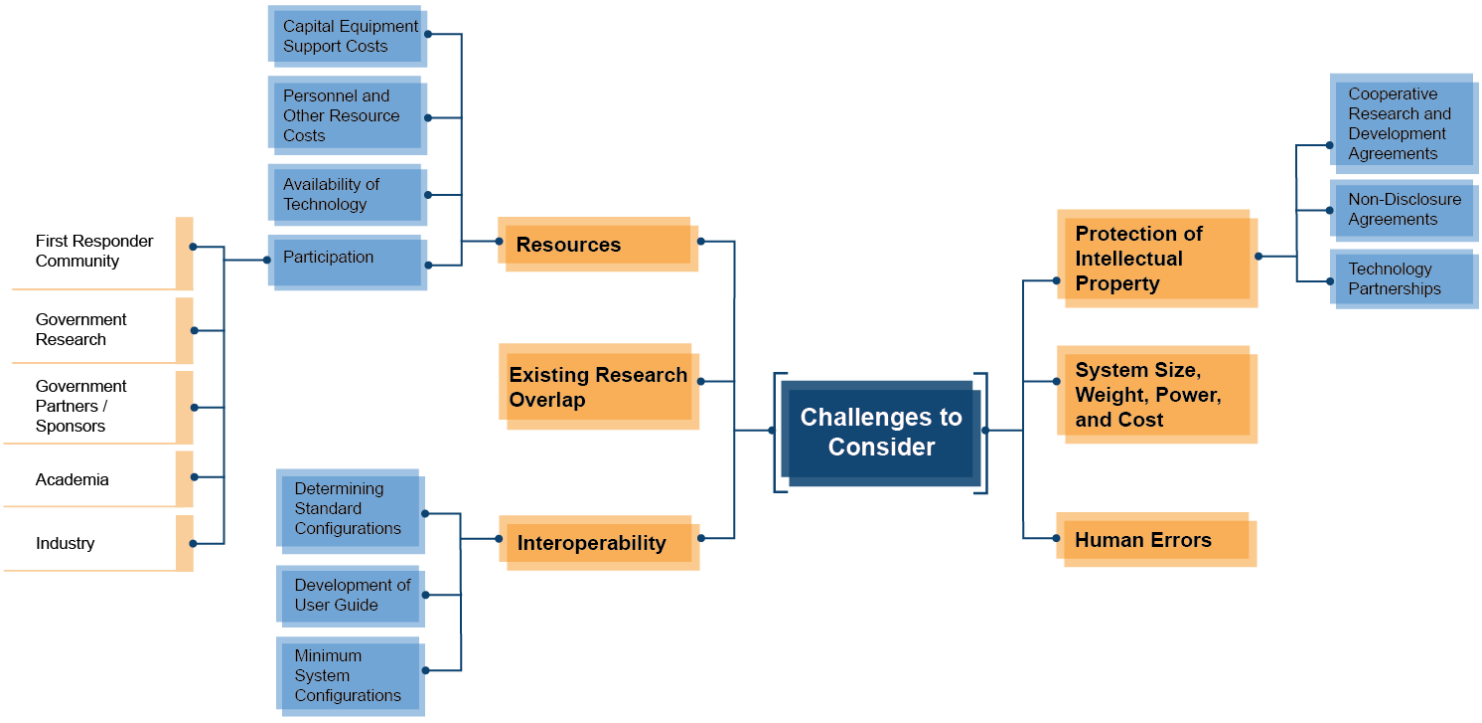
Measurement Approaches / Experiment Design -- *How could research organizations best evaluate the effectiveness of these deployables capabilities?*



Key Performance Indicators -- *What metrics indicate success, effectiveness, or lack thereof for capabilities brought to the testbed?*



Challenges to Consider -- *What challenges may arise when testing identified technologies?*



Next Steps

Continuing with the HMDN project, PSCR will work with DHS S&T to evaluate each technology gap identified in this report to determine the best course of action. Some of the material highlighted may be used as a basis for grant or prize challenges. Other gaps may be investigated within PSCR and addressed through whitepapers and technical reports focused on the specific problem statements, end-to-end solutions, measurement approaches, operational requirements, and standards for each of the four R&D theme areas outlined in this report as it transitions from R&D project planning to project launch. Initial NIST R&D project planning related to Highly Mobile Deployable Networks is currently underway, and more details about specific research initiatives will be announced in 2018. Any research outcomes will be available to the public through the NIST and DHS portals.

For more details on the 2017 Highly Mobile Deployable Networks R&D Summit, please contact Sam Ray (samuel.ray@nist.gov), Maxwell Maurice (maxwell.maurice@nist.gov), or Marc Leh (mleh@corneralliance.com).

Participant List

Name	Organization
Samuel Aden	Michigan Technological University
Mike Bechtol	Rescue 42
John Beltz	PSCR
Richard Bennett	High Tech Forum
Thomas Bilotta	Assured Wireless Corporation
Joseph Boucher	Mutualink
Stephen Braham	Simon Fraser University
Harsha Chenji	Ohio University
Kim Coleman Madsen	Colorado Governor's Office of Information Technology
Ezra Dantowitz	MIT Lincoln Laboratory
Christopher Dennis	PSCR
Ameet Dhillon	Polaris Networks
Cory Dixon	University of Colorado - Boulder
Leonard Edling	Merrionette Park Fire Department
Qumars Eghaneyan	FirstNet
Dan Ericson	Harris Corporation
Matthew Fallows	Trellisware Technologies
Ryan Felts	Corner Alliance / PSCR
Sheila Frankel	NIST
Ed Freeborn	Unmanned Experts, Inc
Victoria Garcia	State of New Mexico - Department of Information Technology
Kevin Gifford	University of Colorado - Boulder
Morgan Gill	FEMA
Vinay Gupta	Polaris Networks
Peter Hallenbeck	Efland Volunteer Fire Department
Joseph Hanna	Directions
Brian Harrison	Baton Rouge Police Department
Nelson Hastings	NIST
Joe Heaps	DOJ National Institute of Justice
Jimi Henderson	Silvus Technologies
Clark Hochgraf	Rochester Institute of Technology
Omneva Issa	ISED Canada
Alison Kahn	NIST
Chris Kindelspire	Grundy County 911
Ezra Kissel	Indiana University
Steve Kropper	Parsloe's Wireless
Robert LaRose	Assured Wireless Corporation
Scott Ledgerwood	NIST
Marc Leh	Corner Alliance / PSCR
Barry Leitch	FirstNet
Kenneth Link Jr.	Monroe Township Fire NJ / State of NJ USAR
Myles Lu	Star Solutions International Inc.

David Luker	East Baton Rouge Parish Sheriff's Office
Cuong Luu	Department of Homeland Security S&T First Responders Group
Terese Manley	NIST / PSCR
Maxwell Maurice	NIST / PSCR
Mick McQuilton	Eagle County, CO
Mark Mendenhall	iCode Mobile Solutions
Gary Monetti	Monetti & Associates, LLC
Zac Mott	Leptron Unmanned Aircraft Systems, Inc.
Bruce Mueller	Motorola Solutions
Michael Murphy	Baker Police Department
Michael Murphy	Neptune Mobile
Kamesh Namduri	University of North Texas
Hien Nguyen	NIST / PSCR
Joseph Nygate	Rochester Institute of Technology
Christine Owen	Oasys IC
Jason Posthuma	Interra
Benjamin Posthuma	NIST / PSCR
Ron Poulin	Codan Radio Communications
Todd Pressley	Oceus Networks
Rolf Preuss	Essential Management Solutions
Sam Ray	NIST / PSCR
John Rowe	Telecom Birddogs, LLC
Vidya Sagar	Spectronn
Gokhan Sahin	Miami University
Charlie Sasser	Georgia Technology Authority
Frederick Scalera	AT&T
Brad Schmidt	Colorado Division of Fire Prevention and Control
Patrick Schwinghammer	FirstNet
Isabel Shaw	Corner Alliance / PSCR
Robert Shuman	Kymeta Corporation
Brian Simons	Persistent Systems
Randy Sisto	Oceus Networks
Bryce Stirton	Responder Ventures
Radu Stoleru	Texas A&M University
Brigido Subiaur	FirstNet
Wyatt Seuss	NIST
Arshad Syed	FirstNet
Jeff Vaughn	Douglas County Sheriff's Office
Britta Voss	NIST
Ryan Wilkerson	AFRL - Rome Research Site
Dan Wills	Sedona Fire District
Darcy Ziegler	Corner Alliance / PSCR