A National Vision for an Inclusive Interoperable Communications Sharing Platform

INTRODUCTION

Despite a decade of significant investments and concerted efforts, a pervasive, national communications interoperability solution for emergency response has remained a bridge too far with, at best, small pockets of interoperable communications ability existing among a few select agencies. Emergency events such as the World Trade Center attacks, the Columbine School shootings, Hurricane Katrina, the Deepwater Horizon oil spill, the Aurora, CO movie theater shootings and host of other natural, accidental and man-made incidents exposed and will continue to expose the persistent and prevailing problem of a lack of effective coordinated communications between first responders and other emergency support and critical infrastructure organizations that are critical to responding to, mitigating and recovering from disasters. Perhaps we have been trying to solve the wrong problem, or at least we have been trying to solve it the wrong way. In this paper, we argue that a broad-based national interoperable communications and multimedia collaboration platform can be achieved quickly and affordably through an everything-over-IP (EOIP) sovereign-controlled, peer-based virtual network. This approach leverages existing communications and media infrastructure as well as next generation broadband efforts, such as FirstNet, to create an adaptive, resilient and scalable collaboration framework that achieves ubiquitous capabilities among first responders as well as critical infrastructure entities.

A BRIEF HISTORY OF COMMUNICATIONS INTEROPERABILITY FOR FIRST RESPONDERS

The issue of a lack of interoperable public safety communications came to the forefront after the events of September 11, 2001. The 9-11 Commission discovered that a lack of interoperable communications between fire and police was a serious problem that hampered evacuations and contributed to the deaths of personnel after the attacks on the World Trade Center buildings[1].

The Department of Homeland Security National Emergency Communications Plan (NECP) defines ''interoperability'' as follows:

''Interoperability-- "The ability of emergency responders to communicate among jurisdictions, disciplines, and levels of government, using a variety of frequency bands, as needed and as authorized..."[2]

The implicit communications capability within this definition is centered on the Land Mobile Radio Service[3], commonly referred to as LMR or two-way radio. Curiously, this definition focuses solely on governmental agencies and their interaction with each other when most other aspects of national policy are explicitly more inclusive. Further, it does not yet specifically address other forms of communications such as real-time video, sensory information, data exchanges, or file/image transfer.

Broadly speaking, DHS-based policies recognize and embrace an inclusive notion of interoperability through a broad-based and scalable inter-agency and inter-jurisdictional collaboration approach to emergency preparedness, response and recovery. Specifically, the National Response Framework (NRF)[4] details how all levels of the government, private companies, and non-government organizations (NGOs) need to be involved in the response to natural and man-made disasters, referred to as an "all-hazards, all-discipline" approach

1 9-11 Commission Report at p.293 http://govinfo.library.unt.edu/911/report/911Report.pdf
2 www.dhs.gov/xlibrary/assets/national_emergency_communications_plan.pdf Appendix 8, page A-26
3 http://en.wikipedia.org/wiki/Land_Mobile_Radio_System
4 http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf

as described in the National Response Framework (NRF)[5] (formerly the National Response Plan (NRP)). This notion of broad-based interdependency and collaborative emergency response is also implemented in DHS's National Infrastructure and Protection Plan (NIPP)[6] through its doctrine regarding Critical Infrastructure and Key Resources (CIKR), which categorizes 18 "all discipline sectors", as well as in the National Incident Management System (NIMS)[7]. Mr. Craig Fugate, the Administrator of the Federal Emergency Management Agency (FEMA), in congressional testimony, said "Government can and will continue to serve disaster survivors. However, we fully recognize that a government-centric approach to disaster management will not be enough to meet the challenges posed by a catastrophic incident. That is why we must fully engage our entire societal capacity...."[8]

Over the years, various approaches have been implemented to address the interoperability problem as defined by DHS. Virtually all are in use today. To some degree, these systems address certain aspects of the interoperability problem, but none contemplate an inclusive national capability. The inclusion of other public agencies and private enterprises was largely ignored by these solutions, following the notion that incident response was the sole responsibility of first responder agencies. Furthermore, their focus was primarily on technology rather than on the underlying problem and the desired end result. In this case, interoperability is not the fundamental goal. Instead, classically defined interoperability is just one of the requirements to meet the national policy goals of inclusive, broad-based communications collaboration to enable all relevant organizations to prepare for, respond to, and recover from incidents in a coordinated and collaborative manner.

Given the articulated national goals, an interoperability solution must address three fundamental areas involving collaboration: 1) who should be involved, 2) how they will be able to communicate and exchange information in order to effectively collaborate and formulate responses, and 3) most importantly, how do you make the universe of potential network members willing to participate in the first place in light of massively diverse legacy infrastructure, limited financial resources, as well as issues of sovereign control, privacy and differing responsibilities and primary objectives

In fairness, the problem is massively complex. National policy as described in the NRF, NIPP, PPD8[9], NIMS, etc. (and logic) contemplate close collaboration and coordinated efforts among first responder agencies and critical community partners both in preparation for, response to and recovery from emergencies of all types. This concept is encapsulated in the notion of a scalable, all-hazards and all-disciplines approach to emergencies. This type of multi-agency and community partner interaction necessitates a level of connectivity among and between potential incident participants and their varied communication assets that calls for a very different approach to those undertaken to date.

THE CHALLENGES

Let us first look at some of the challenges. Tremendous amounts of communications media infrastructure (radio, video, mobile communications, sensory information, telephony, data files and chat) exist in disconnected silos in both vertical (large hierarchical organizations) and across horizontal (cross-agency, critical infrastructure partners) environments. Usually, all of these varied communications and media assets are controlled by their respective owners, whether they are local, state or federal sovereign government entities or private owners. Each of these owners is unlikely to relinquish control over its critical communication resources to other entities. Furthermore, these sovereign owners are not likely to share their information and communications resources in an environment that is not secure. Many valid reasons exist for maintaining control of communication

5 http://en.wikipedia.org/wiki/National_Response_Plan
6 http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf
7 http://www.fema.gov/emergency/nims/
8 Administrator Craig Fugate, Federal Emergency Management Agency, before the United States House Transportation and Infrastructure Committee, Subcommittee on Economic Development, Public Buildings, and Emergency Management at the Rayburn House Office Building, March 30, 2011.
9 http://www.fema.gov/ppd8

assets that range from privacy issues, regulatory restrictions and mandates, differing jurisdictional and functional responsibilities, different stakeholders and political implications, among numerous others. This mosaic of interests is further complicated by the nature of the subject matter itself.

Emergencies are unpredictable, and the nature of risk dictates that one does not know with whom he will need to coordinate, where that person is or what form of communications and information will be required to mitigate the issues that arise. Additionally, emergency environments are not static events; new primary as well as secondary and tertiary effects can rapidly emerge. Therefore, communications are needed with those both in immediate proximity and with those considerably more remote. The real world exists in an infinite number of intersecting concentric circles with complex inter-dependencies; perhaps our approach to communications should reflect this reality. Additionally, the individuals who are tasked with running these communication systems are themselves bandwidth challenged with the increasing complexity of technology that they are required to master while all the time facing tighter and tighter budgets.

Traditional approaches to these communication challenges focus mainly on "interoperability" for a small subset of the necessary participants. The problem with how classic interoperability addresses this complex problem is multifold. Interoperability, defined as one system communicating with another at the system level, is non-scalable in horizontal environments and it certainly does not contemplate the notions of infinite intersecting concentric circles or the dynamic and unpredictable nature of risk and response. Of equal importance, these solutions are by their nature non-inclusive, only addressing the problems of some traditional first responders or other public sector entities (e.g., P25 radio networks), excluding most of the universe of necessary participants. Other approaches have featured architecture that breaches the sovereignty and/or security requirements of other communication resource owners, dooming them to lack of adoption from inception.

From a problem-solving perspective, all of these interoperability approaches share a common yet faulty presumption; that figuring out with whom you are most likely to communicate can solve the problem. While this may be a logical and practical approach on the surface, it perpetuates the mistakes which lie at the heart of the complexity of problems. If we were able to predict the nature, scope and collateral effects of any disaster, then there would be no need to respond because they could be predicted and mitigated in advance. The truth is much more complicated; the true scope and risks of any disaster extend in untold numbers of directions as viewed from any number of different but interconnected perspectives. A new approach to this complex problem is needed to begin to solve this issue on a national level once and for all.

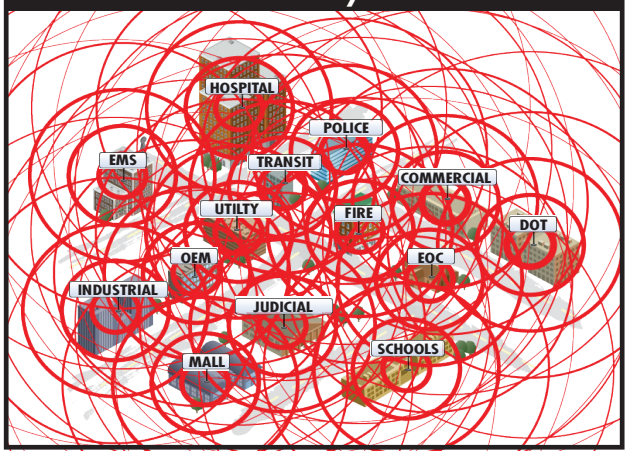
A BETTER APPROACH - COMMUNICATION RESOURCE SHARING VS. INTEROPERABILITY

If classic silo interoperability is not the answer, perhaps a new notion of interoperability that contemplates the critical issues outlined above is the solution. This new notion of interoperability is really more about sharing communication resources than it is about getting all of these diverse systems from diverse and geographically dislocated owners to agree en masse to communicate and interact down to the systems and event scenario level. Communication resource sharing allows one entity (or multiple entities) to securely hear, talk with and share information with other entities as required, irrespective of who those entities are or where they physically reside or what forms of media and content they chose to use.

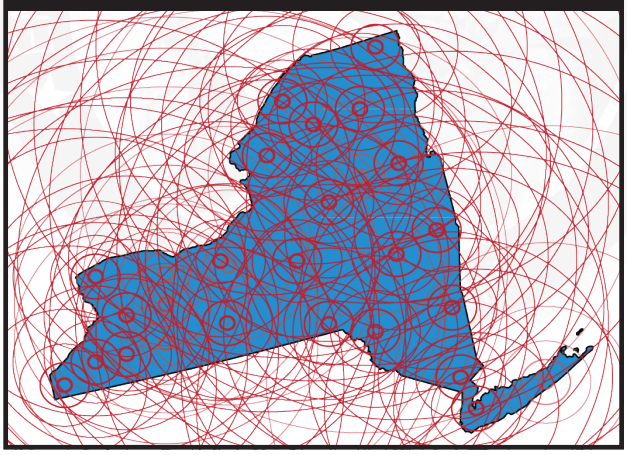
APPLICATIONS AND CAPABILITIES

As noted above, the result of previous, well-intentioned efforts is a mish-mash of unconnected silos (non-intersecting non-concentric circles) of applications. Applications solve only small slices of this overall issue and prevent the required ubiquity. What is needed are efforts to unite these silos and transform them into a national capability. A capability that allows the right information to get to the right people at the right time must necessarily be unlimited in scale to effectively embrace the notion of intersecting concentric circles; similarly, this capability must also allow any combination of participants and communications resource types to come together in an ad hoc fashion to respond to the demands of unpredictability.

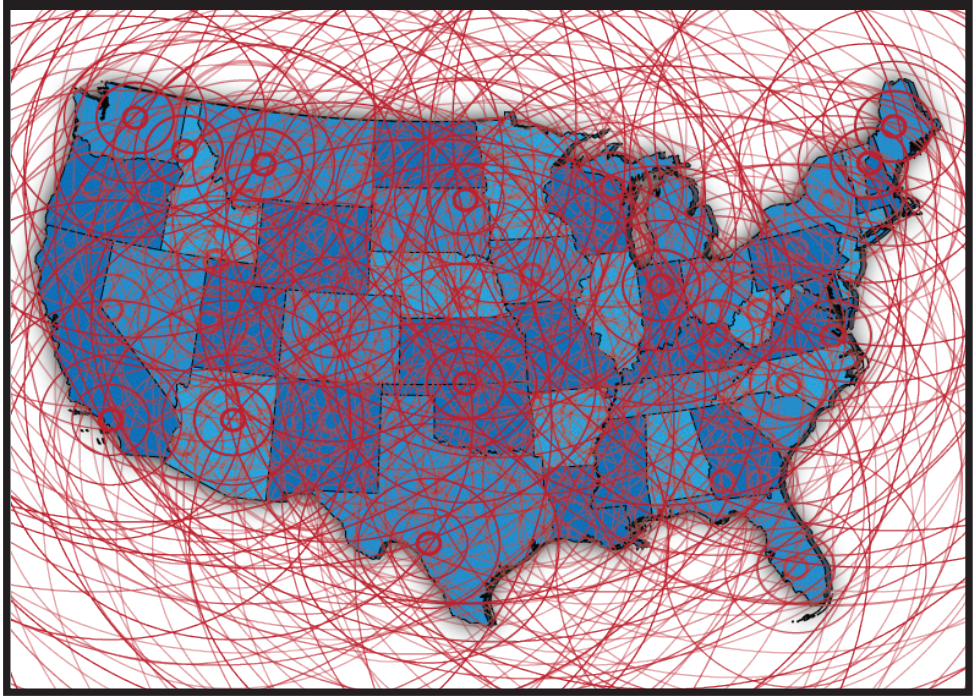
View of Community-Wide IRAPP



View of State-Wide IRAPP



View of Nation-Wide IRAPP



PIPES AND MEDIA

Simplistically viewed, communications can be viewed in two overall categories, pipes and media; pipes being the transport methodology and media being the content and applications that do or could ride on those pipes. Substantial resources have gone into developing world-class transport networks and media and content of every imaginable stripe. Similar investment is needed to bring that entire media onto all of those pipes in a secure fashion, respectful of the sovereignty of its owner, so they are willing to share it, at will, among and across the spectrum of relevant participants.

LTE: A TREMENDOUS EVOLUTION, BUT WE CAN DO EVEN MORE

The initiative around LTE allocates a "big, fat, fast" pipe to first responders and will enable substantial multimedia communication among first responders as media is developed and adapted for that pipe. This initiative can be taken even further by making the overall strategy more inclusive. As we have articulated, national policy (PPD8, NIPP, etc.) is quite inclusive, so let's be sure to advocate technology solutions that are also inclusive. LTE is an important part of the national capability being advocated in this paper, but it is only a part. The addition of the capabilities and broad participation being put forth in this paper will make LTE stronger and align technology with policy. Only by focusing on the desired end state of national policy, that of an inclusive, ubiquitous national capability, will we, as a nation, finally put this challenge behind us.

NO MIDDLE, NO PROBLEM; OR PROTECTING SOVEREIGNTY THROUGH ARCHITECTURE

Two of the primary and substantial challenges in making entities willing to participate in multi-agency interoperable environments are: respecting the sovereignty of their communication resources and ensuring a secure environment over which those resources may be shared. One way that the sovereignty of control of resources can be assured is through the fundamental architecture of the system that connects them. A classic approach to communication network design is the "hub and spoke". While this can certainly be a fine technical solution, it does not address some of the key human challenges to attaining a multi-agency interoperable communications environment. Principally, it does not respect the sovereignty of the individual participants' own communications assets because one of the entities is hierarchically superior (hub) to the others (spokes). If, in such a system, one were to remove the controlling central hub and place the control and intelligence of the system out at the (their) edge, proximate to each of the owners of the various communication resources, a network of peers would emerge, substantially mitigating concerns regarding control sovereignty. Furthermore, in this peer-to-peer[10] environment, through technology, each communication endpoint device is knowledgeable of all other endpoints and knows how to directly reach them and establish a communications path between them without the aid of an intermediary host server. As for the issue of security, it can be addressed in three categories: platform or operating system (OS); validation of participants; and transport mechanism. An environment having a secure OS, utilizing a dynamic Public Key Infrastructure (PKI)[11] to mutually and securely validate participants, and wrapping the transport in encrypted tunnels would address security concerns of the participants. Taken together, these technical attributes serve as the foundation upon which a large-scale capability can be built.

THE LOWEST COMMON DENOMINATOR AND ENABLING YOUR MEDIA

From a problem-solving perspective, what if, as opposed to trying to figure out who needs to talk to whom and then implementing a series of separate application silos, this problem set was approached from the perspective of the lowest common denominator, with communications media being the lowest common denominator? What if, instead, all of this various media were simply enabled from where it is concentrated onto a secure network that respects the sovereignty and security concerns of the owners of the media, resulting in, not a series of discrete applications, but instead a distributed but unified capability? It is suggested that many previously daunting, and perhaps unrelated, communication challenges will fade away if this approach is adopted. Individuals from within complex entities and among unrelated entities making the same decision, to simply enable their media, will solve more problems than they set out to solve.

MAKE IT EASY AND AFFORDABLE

With the increasing complexity of technology it becomes more and more incumbent upon the maker of technology to make the user experience as simple and intuitive as possible so that the value of the technology is not lost through cumbersome interfaces. Additionally, as cost is always a consideration and in order to have the participation of all the relevant entities; a solution priced low enough could attain viral attributes.

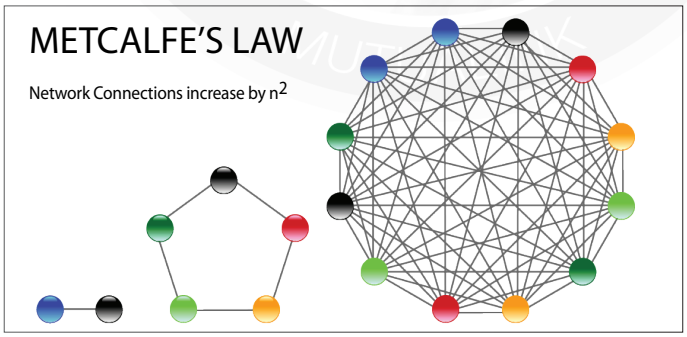
10 http://en.wikipedia.org/wiki/Peer-to-peer
11 http://en.wikipedia.org/wiki/Public_key_infrastructure

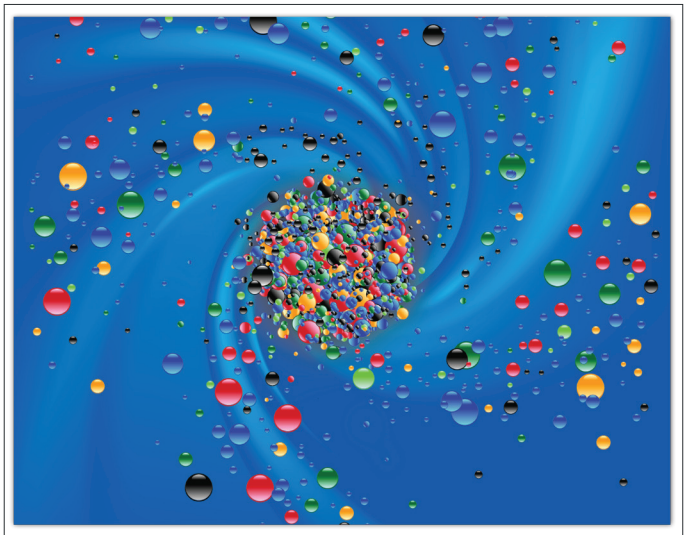
YOU MEAN I DON'T NEED A LAWYER?

In our peer, media-enabled communications environment, there emerges another benefit. In order to engage in an ad hoc multi-agency communications session, someone needs to be invited (or to invite someone). This invitation and acceptance mode of operation eliminates the need for traditional Memorandums of Understanding (MoU)[12]. Historically, MoU's have been used between agencies to articulate the circumstances under which these various communication resources can be "tied" together; this is due to the centralized nature of the traditional hierarchical architecture that was used. In our new evolutionary model, the MoU is not necessary because each individual session invitation and acceptance serves as a rolling MoU.

THE EMERGING NETWORK FACTOR

As this concept of securely enabled media is adopted, it becomes clear that the old axiom of Metcalfe's law - "the value of a telecommunications network is proportional to the square of the number of connected users of the system" - is also true for the world of interoperable communications. Imagine being presented with this choice; you are the communications coordinator for your county and you wish to unify communications of the towns within your county. You are presented with two options: the first communication system fulfills your initial goal of unifying the communication within your county's government agencies and only your county; the second communication system will provide the same functionality but will also allow secure and sovereign communication with private sector assets within your community, and both public and private sector assets in surrounding communities and beyond. Both are the same price, which would you buy?





Metcalfe's Law defines network growth. Participants gravitate toward an ever-increasing network.

THE FALLACY OF THE COMMON OPERATING PICTURE

The notion of a Common Operating Picture (COP) is most often a fallacy; there are really only operating pictures. Each entity involved in incident resolution has its own unique and important perspective of that incident, so for any incident underway there are many operating pictures. Perhaps there is a COP from any number of intra-departmental perspectives, but there is likely not one from an incident-wide inter-departmental perspective. If the individual agencies involved in the incident enabled the media that is their operating picture, their media, too, could be shared with other incident participants, creating a true COP.

12 http://en.wikipedia.org/wiki/Memorandum_of_understanding

A NATIONAL VISION FOR AN INTEROPERABLE RESPONSE & PREPAREDNESS PLATFORM (IRAPP)

As was just articulated, the need is known, the policy exists, the participants have been identified, the challenges understood, and the technology now exists to create a national capability that securely unites the communication resources of those charged with protecting life and property from both the public and private sectors onto a national Interoperable Response And Preparedness Platform (IRAPP). The IRAPP's inherent capabilities allow new, existing, and vintage communication systems to share communication resources through a methodology of securing existing terrestrial and wireless IP-based networks.

IRAPP IN ACTION TODAY

The IRAPP concept is being embraced today on both coasts in several large metropolitan areas, including the State of New Jersey and the Northern California Bay Region. One practical example of interagency, multimedia interoperable communication resource sharing took place in Jersey City, New Jersey during the recovery operations of US Airways Flight 1549, "Miracle on the Hudson"[13] plane crash. Jersey City first responders were able to share live video and voice communications they had previously enabled from their harbor side cameras and their Emergency Operation Center with a number of area hospitals and public safety organizations allowing each entity to assess the situation and plan their response accordingly. Key to the success of the communications response to this incident was that Jersey City proactively chose, and encouraged others to join an inclusive system while ensuring it was regularly used and exercised so when the crisis hit there was no hesitation in turning to it.

The momentum for a national secure multimedia communication resource sharing capability is growing throughout the Country. The Northern California Regional Intelligence Center sponsors an alliance of agencies and private sector entities that share information and collaborate in real time on a daily basis. In New Jersey, hospitals, casinos, malls, schools, transits, municipalities, etc. and first responders participate in the same always on, always ready virtual network referenced in the Miracle on the Hudson incident as cited above. Like New Jersey, the Bay Area, and other growing regions in the US, there is no longer a reason why every community in our country can not have agencies and key infrastructure seamlessly communicating and collaborating in real time during times of crisis. National multi-media interoperability and resource sharing can be achieved immediately with the Mutualink system; the key to this effort starts with community leaders being willing to transform their communities for the good, in a simple yet powerfully effective way. With Mutualink, interoperability is achieved without complex and costly large-scale communications projects. Instead, a new transformative and incremental approach can be taken that catapults communities forward. Through these many acts of community leadership, a national fabric will be woven into existence solving our nation's emergency communications challenges.

13 http://en.wikipedia.org/wiki/Miracle_on_the_Hudson

Mutualink, Inc.

Connecticut Headquarters
1269 South Broad Street
2nd Floor
Wallingford, CT 06492

Research & Development
3 Lan Drive
2nd Floor
Westford, MA 01886

Development Facility
Guanajibo Industrial Park
2015 Jaime Rodríguez - Suite 3
Mayagüez, PR 00682

Phone: (866) 957-5465

E-Mail: info@mutualink.net

Web: www.mutualink.net