

A grayscale photograph showing the silhouette of a soldier in profile, wearing a helmet and tactical gear. The soldier is positioned in the foreground, looking towards the right. In the background, the stars and stripes of the American flag are visible, slightly out of focus. The overall tone is somber and professional.

Blueforce White Paper

Information Mobility: Collaboration and Shared Situational Awareness for Last Tactical Mile Operations

Written by Michael Helfrich - February 2011

Blueforce Development Corporation

217 essex street, suite 22 • salem, ma. usa 01970
phone: 866.960.0204

Information Mobility: Collaboration and Shared Situational Awareness for Last Tactical Mile Operations

Written by Michael Helfrich, Blueforce Development Corporation

THE CHANGING THREAT MODEL

Some would consider it a luxury to have the security challenges of our parent's generation. It was a time of known adversaries, "battle fronts", and nation-state actors. The 20th century "mass and maneuver" platform-centric model of our parent's day has been replaced with an asymmetric threat model where a network-centric concept of operations must be adopted because chaos and non-predictiveness has replaced past eras of order; where today's coalition or inter-agency workgroup presents a different membership tomorrow. Operational approaches require the complete and total embrace of tactics and technology that address the ultimate in complex adaptive systems where we operate and interoperate in denied, dysfunctional, and disparate last tactical mile environments.

Religious fanatics, non-nation state actors, and ideological adversaries don't face us head on; they sneak up and attack using small units simultaneously and at multiple locations. The strategy and tactics of "asymmetric warfare" is best personified with the attacks in Mumbai: ten shooters took a major city hostage for an extended period of time by mounting attacks in multiple locations with extreme lethality. Even more troubling was the attackers' use of highly available mobile devices, internet tools, and social networks: it has become apparent that the Mumbai attackers were adept in the effective use of the "mobile internet" for their own command, control, and communications tactics as they swarmed throughout the city.

Welcome to the age of the "mobile Internet", where fixed infrastructure and mobile, ad-hoc wireless networks provide connectivity across the "battle space". Despite this pervasive connectivity, we continue to hear stories about the lack of information and/or information breakdowns because of interoperability issues amongst information applications. While some of these issues are rooted in policy and culture, commercial-off-the-shelf (COTS) technology exists today that enables these last tactical mile teams to rapidly form, securely share actionable information, and do so in an interoperable fashion that ensures success against today's threats and provides a higher level of situational awareness across the entire information value-chain, vertically and horizontally. The Mumbai attackers demonstrated this thesis.

Whether the conflict is in Mumbai, London, Bali, or New York City, one thing is certain: Decentralized and non-predictive threats require us to rethink and rapidly adapt our tactics, information flows, and tactical technologies to support new mitigation and response models for those working in "last tactical mile" or "edge" environments. Enabling the sharing of actionable information amongst "edge" operators is the lynchpin of a network-centric operational model which enables organizations to create and share information to increase tactical advantage through the rapid formation and collaboration of small, agile, and empowered self-directed teams using mobile technologies. The mobile internet will be a transformational piece of this equation.

INFORMATION MOBILITY: JET FUEL FOR MISSION SUCCESS

There is a “half-life” for information and it degrades as a function of time, yet having the right information is often the discriminator between mission success and mission failure. Given the stochastic nature of agency “swarms” that will mitigate and respond to hostile acts, it is imperative that network centric systems allow for the effective exchange of information amongst components, agencies, coalition partners, foreign governments, and international organizations as they are critical elements needed to defend the nation and execute national strategy.

The changing nature of 21st century conflict forces us to rethink the information domain. Each domain has its own set of information and unique operational requirements that must be considered. This paper will reference three information domains that are relevant to the discussion:

- **Center:** The “center” is comprised of hardened facilities which house data centers, IT support staff, and pervasive network connectivity. The “center” is often exemplified by Fusion Centers and/or Headquarters functions which are monitoring and managing multiple swarms.
- **Near-Edge:** The “near edge” is located very close to the action. Commanders and unit leaders are often housed here and receive/promote information to/from the “far edge” and to the “center”. Network Centric doctrine pushes decision making to these constituents as they are much closer to the action and have better situational awareness of “far edge” action. The “near edge” is often exemplified by Command Posts (CP), Tactical Operations Centers (TOC), and Forward Operating Bases (FOB).
- **Far Edge/Last Tactical Mile:** Those in the “last tactical mile” or at the “edge” are executing the action. Those that work in this space can be characterized as carrying weapons, hoses, and/or sporting badges. Extreme mobility is the requirement here and access to, and the ability to share, information is mission critical and core to life safety.

As national security agencies and commands have begun to make the shift towards a network-centric environment, information continues to be handled using highly verticalized paths and processes, hence the phrase “silos of information”. It is this verticalized, exclusively edge-to-center movement that turns actionable information into stale information. Indeed, information should always end up in the “center”, but mechanisms and technologies must exist that provides for rapid formation of teams and for secure, agile, and adaptive sharing of information when and where it is needed most. A hybrid vertical and horizontal collaboration model enables mobile teams living at the edge to accomplish their missions while also serving the needs of the information enterprise and communities of interest that live at the center.

To truly enable the edge to create, share, and pulse around actionable information, a strategy that embraces “information mobility” must be embraced. Information mobility provides for a dynamic availability and sharing of information which is governed by business rules, standards-based interfaces, interoperable protocols, mobile platforms, and guidance/policy to address the needs of both planned and unanticipated information sharing events. Information mobility is the foundation for shared and user-defined situational awareness in the last tactical mile, but also across the information enterprise.

The resultant benefits of enabling transparent, open, agile, timely, relevant, and trusted information mobility and situational awareness amongst highly mobile small units and their command staff can be best summed up as follows:

1. Self-synchronization and unity of effort across mission, inter-agency, and coalition operations
2. Mission efficiency and increased operational tempo because of resultant speed and execution of decisions
3. Rapid mission adaptation through interoperability across mission and coalition operations
4. Situational precision through an ability to anticipate events and resource needs, providing an initial situational advantage and setting the conditions for success.

TODAYS CHALLENGES

For last tactical mile teams, today's notion of information mobility is largely the domain of voice traffic. For years, radios were the "killer app" for the movement of voice. More recently, radios have been augmented with cell phones because the latter provides native interoperability through existing "plain old telephone system" (POTS) infrastructure. It is clear that six years after Hurricane Katrina, the notion of "radios, "interoperability", and "coalition" remains an oxymoron, despite the billions of dollars expended at finding a solution.

There are early indicators that public and private sector organizations are shifting from RF-based voice communications to internet-based solutions for the movement of voice. Voice-over-Internet-Protocol (VoIP) technologies are evolving such that they are now a viable solution to the problem. With this shift comes the tacit recognition that voice is but one "data type" that the mobile internet can carry: the same channels that carry VoIP traffic can also be used to move and share much richer and more contextualized situational presence information such as geolocation, interior location, biotelemetry, images, floor plans, and sensor data.

Applications for mobile devices that provide a richer view of the mission space are emerging with the advent of several blockbuster handheld platforms such as Android and the iPhone. While the emergence of these applications provides much needed tools for the movement of rich incident data, problems remain because of the focus on "micro-application" architectures, single-user viewpoints (e.g., non-collaborative and non-social), lack of security, and a continued lack of support for interoperable protocols and transports. Instead of the single "silo" and "black box" that voice products yielded, we are now faced with MANY silos and black boxes because of the single dimension of micro-applications.

A little over a year ago, a U.S. Department of Defense Special Operations Commander lamented about the current state of the wide array of information tools taken into the fight. He referenced 24 discrete information tools, each with their own exfil, each using proprietary protocols, each with differing support for crypto, and each with its own application to collect and consume the data. Each system provides value to the mission, but that value is lost because decision makers must toggle between systems, creating a disjointed operational view and decaying the timeliness of actionable information.

What is needed is an integrated mobile application framework that fuses information about, and between, endpoints in a highly just-in-time, and secure fashion.

BLUEFORCE TACTICAL: FUSED, SECURE, AND INTEROPERABLE COLLABORATION AND SITUATIONAL PRESENCE

Blueforce Tactical (B-TAC), a patent-pending mobile software application for Windows Mobile Smartphones and PDAs (soon on Android and iPhone/iPad), provides a mission critical solution for life safety, mission efficiency, and the movement of perishable tactical mission data amongst team members and commanders. The software provides an ultra-secure collaborative framework for the exchange of information, telemetry, and person-attached sensor data amongst individual participants engaged in situational intelligence gathering, tactical missions, and decision support activities.

B-TAC was designed and built using a “need-to-know” technology model, while still facilitating the rapid formation of agency and/or inter-agency workgroups. B-TAC’s extensible “plug-in” architecture provides for integration with a multitude of handset platforms, sensor types, and information services. The software enforces secure information exchange between each trusted participant using NSA-certified (FIPS 140-2 and Common Criteria EAL2) cryptographic protocols and rides on standard cellular, WIFI, WiMAX, satellite, and/or ad-hoc wireless mesh networks.

B-TAC’s Tactical Presence Protocol fuses geo-location, network location, health, and sensor data into a presence heartbeat that is light on the network, yet provides complete tactical awareness as to where your people are and what’s going on around them. These core services, which are fused and selectively shared amongst those whom each endpoint allows, include:

- **Collaboration:** B-TAC provides for information exchange that enables the rapid sharing of incident information through the use of unstructured text, images, files, or text messages. These messages originate from other B-TAC users working in the area, or from a command post or an emergency operations center using a Blueforce Fusion node, and may include imagery, mugshots, building floor plans, and/or other critical mission information.
- **Location Awareness:** With built-in GPS parsing, B-TAC enables users to share their location amongst subscribers using the NMEA-based GPS receivers built into handheld units, or accessed using Bluetooth interfaces.
- **Network Awareness:** For WIFI and WiMAX environments, B-TAC can constantly monitor the ID tags of the wireless access points (WAPs) it uses to communicate, but also “hears” around it. Based on the signal strength of the WAPs the software “sees” in the area of operation, B-TAC can transmit proximity metrics to track personnel based on their network proximity. This is useful for interior situations, but also for signal intelligence, collection, and exploitation activities.
- **Sensor Awareness:** B-TAC provides a plug-in interface that allows person-attached sensors and their data to be fused into the awareness protocol and shared amongst subscribers. Sensors that have been integrated to date include chemical (blister and nerve), passive infrared/heat, seismic, explosive, acoustic, magnetometer, gyroscope, accelerometer, heart rate, respiration, pulseOx,

and streaming/static JPEG imagery. The plug-in architecture provides for a four-state “flag” to trigger alerts and alarms. The product also features a “panic button” that allows the responder to punch two keys which trips a panic indicator which will cause all B-TAC devices in the area to alarm that someone near is in danger and in need of assistance.

- Network Adaptive: B-TAC works with wide area networks (WANs) where XML message switches are used to route B-TAC data. Many incident scenes may not have wide-area connectivity or are hindered by network environments that introduce jitter and intermittent connectivity. B-TAC will work on ad-hoc LANs where no servers are available, allowing users to communicate point-to-point using ad-hoc wireless “bubbles”.

THE WAY FORWARD

Events since 2001 make it quite clear that asymmetric threat models are here to stay. Consistent with that model is the need to facilitate small-unit swarming and horizontal sharing of actionable information so as to enable superior decision-making amongst those working in the last tactical mile. Prevention, mitigation, and response protocols will require rapid adaptation given the stochastic nature of threat events. An ability to leverage highly mobile devices, riding on fixed or ad-hoc wireless clouds is critical to moving actionable information amongst those working in national security mission spaces.

Core to the goal of information superiority is adopting strategies and tactics that truly enable “information mobility” up, down, and across the tactical mission space. Perishable information must be shared in a timely manner so as to affect life safety, mission optimization, and decision superiority. Information mobility ensures that actionable info is shared at the right time, and in a highly horizontal fashion, such that those with the power to act can do so decisively. Information mobility strategy and tactics must deviate from today’s technologies that force deterministic, fixed, and permission-based interactions in highly vertical and stove-piped silos.

With this horizontal movement of actionable information comes the tacit recognition that inter-agency and coalition partners must be considered. Furthermore, only integrated mobile applications that ensure data interoperability (to include voice), support for fused sensor data, and provide an extensible application framework that is adaptive to mission membership and function will make information mobility a reality.

Blueforce Tactical delivers on this promise today by enabling a more dynamic, more adaptive, higher-speed “response” team that leverages the collective capabilities of all the participants. B-TAC software helps mitigate many of these challenges by providing rich, secure, and distributed tactical awareness that helps teams locate, identify, and leverage resources using a computing and communications device that matches the environmental and the operational requirements they work under: mobile, un-tethered wireless handheld devices.