# The International Heartbeat Beacon for interoperability & synchronicity of event, alert data

**Steven McGee**
SAW Concepts LLC
stevenjmcgee@sawconcepts.com

**Reverend Kathy Graves**
Kathy's Rainbow Reiki
kathysrainbow@mailstation.com

## ABSTRACT

The Heartbeat Beacon addresses data temporal / exchange interoperability gaps by stipulating CAP instantiated data exchanges for military, first responder, and commercial stake holder domains by standardizing data exchange formats, symbol sets, event refresh rates enabling direct collaboration with military telemetry systems using commercial products. Multicast radius will be adjustable e.g., increase / decrease with audible tones based on business logic / military mission thread logic according to threshold rules visually displayed as concentric color band expansion / collapse based on DHS five level color / audible advisory schemes. Alert, evacuation, alternate routing of transportation assets, medical triage will then are adjustable. Organizations through router/switch updates via heartbeat messages will enable spontaneous integration of disparate communities of interest allowing the network to be maneuvered in response to unified events and alerts.

### Keywords

Heartbeat, Beacon, TCP/IP, heartbeat sub-protocol, synchronicity, interoperability, Public Safety Answering Points – PSAPS, e9-1-1 next generation, network management, forensic network analysis, procedure, method, maneuver the network, spontaneous integration, commercialize network centric warfare

## BACKGROUND

A congressional directive states "nothing less than network centric homeland security akin to network centric warfare". Federal / military situational awareness (SA) SATCOM, Telco / cable networks supporting First Responder e9-1-1 systems apply 3 common denominators: the TCP/IP heartbeat protocol, heartbeat transponder beacons & heartbeat (XML) schemas / messages conveying network configuration data e.g, router MIBs: multicast group subscriptions -- DIFFERENTLY. As shown in the below inserted graphic; the Heartbeat Beacon addresses the data / temporal / symbolic interoperability challenge where unique / proprietary federal / military situational awareness (SA) systems and Telco networks supporting First Responder systems agree on common, settings of three common denominators and four focus areas:

I TCP/IP heartbeat protocol state data commonly timed, harvested & broadcast via beacon transponders.

II Heartbeat network (re) configuration XML schemas / messages Efficient/BREW/SWIFT, binary... XML formatted small data files replacing military unique Tactical Data Link / Joint Variable Message Formats.

III Common Alert Protocol CAP child schemas / data islands as a single, unified trigger for alerts

Four Focus Areas:

I Establishment of consistent timing and synchronous state meta-data collection using the heartbeat / beacon's intrinsic millisecond - 99 minute timing function to enable consistent, synchronized collection of raw state meta data (geo location, moving, halt, IP address, unit / organization Universal ID) BEFORE transfer to queues, SANS, dbase... prior to data fusion activities improving filtering / intel fusion.

II "Maneuver the network" Use collected state meta data enabling network management of router Management Information Bases MIBs installing network router MIB updates for spontaneous (re) organization split,

join, adds via multicast - anycast broadcasts of heartbeat harvested state meta data (geospatial location, status: moving, halt, URN, Org ID, Universal ID…)

III Instantiate chopchain - workflows – business logic over multicast / anycast IP using "true cots" tools in use i.e., Towersoft w/AgileDelta Efficient XML module embedded via the Common Alert Protocol CAP (XML child schemas and or data islands / embedded files ) to support the multicast, unicast/or anycast distribution of events, alerts via a unified alert / event trigger mechanism – the OASIS Common Alert Protocol with child schemas and / or data islands to accommodate disparate Communities of Interest (COI's)

IV Apply beacon technology to enable millisecond data exchanges vice 30 second screen scrapes while increasing / decreasing radius of disaster / event / alert radius represented by multicast zones corresponding to US / UK... five level advisory systems Enable across N complex systems, Y networks and Z.

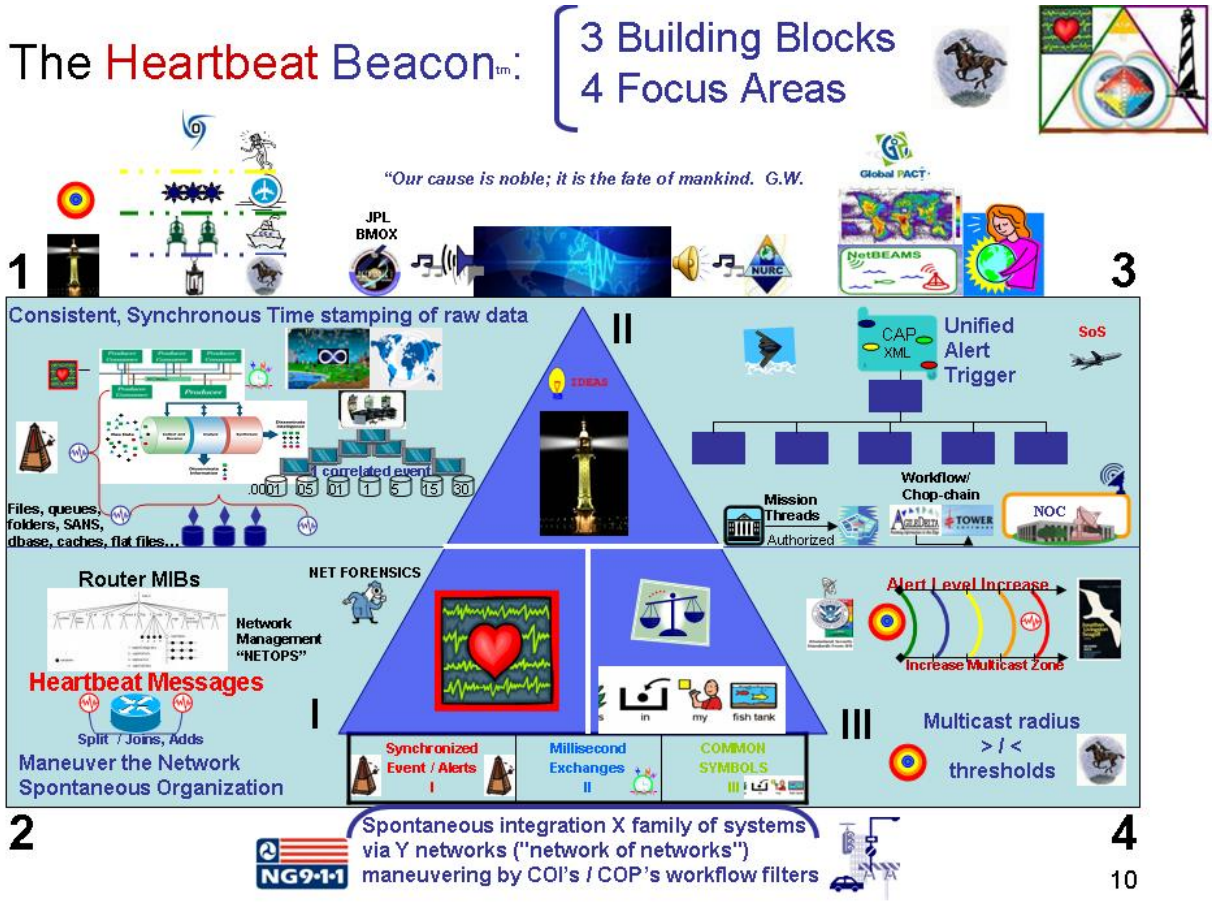


**Figure 1. 3 Common Building Blocks / 4 Focus Areas**

Uses of the heartbeat beacon range from calling in help, bringing in teams, groups, logistics support, and subject matter experts to a crisis zone defined by community of interest described alert and event thresholds. The opposite, evacuating areas based on thresholds and types of events and alerts – say a Tsunami, is achieved by sensors located on buoys on the ocean's surface and floor sampled in the millisecond to 99 minute range enabling an estimate of coastal areas impacted. After the Katrina disaster, the council of Mayors agreed that military involvement was needed as soon as possible. Applying three common denominators in four focus areas is a simple solution. Apples to apples and oranges to oranges collaboration is improved by the heartbeat beacon methodology in establishing

common symbol sets, synchronous data refresh rates designed to not saturate limited available bandwidth or too slow refresh rates resulting in overcome by events reporting.

The military tends to handle network mobility more efficiently than the commercial sector having established a procedure to harvest network state information about their organizations that translate to moving units from network subnets based on operational need. Since routers work the same way whether purchased by the military or mayors, the heartbeat beacon's methodology will enable organizations and military units to organize for a common cause by tethering and untethering to networks in an adhoc yet purposeful manner. Since response involves dispersal of funds, the Heartbeat Beacon will also serve to notify communities that funds have been transferred or released to a disaster zone. The FBI deployed a team to monitor financial transaction data stores following 9/11. Gathering state meta data from target platforms, hosts and subnet or cells of interest (e.g., the function of the DHS's TRIPWIRE shown in the lower left hand quadrant IV in figure 2 below); will serve to notify units of action (UA) in military speak to converge on suspected terrorist financial activity. Teams monitoring financial activity (i.e., a core CIA activity) will be synchronized with teams responsible for physical detainment and arrests. The concept involves spontaneous integration of a CIA or FBI anti-terrorism squad using the SWIFT based Terrorist Finance Tracking Program. The Terrorist Finance Tracking Program is a United States government program to access the SWIFT transaction database, revealed by *The New York Times* in June 2006. It is part of the Bush administration's "Global War on Terrorism". Based in Belgium, SWIFT (Society for Worldwide Interbank Financial Telecommunication) establishes common standards for financial transactions worldwide.

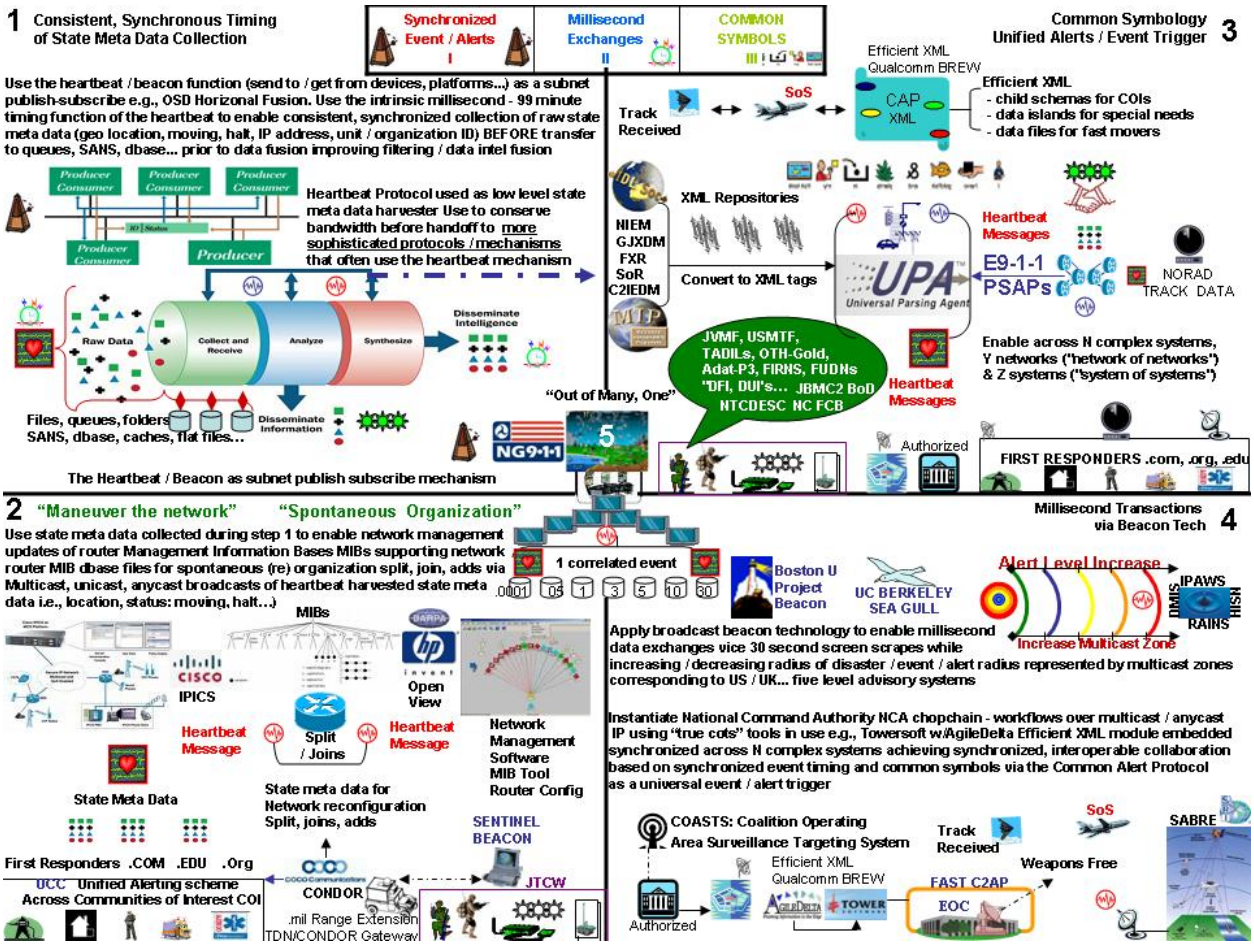


**Figure 2: Focus Area Quad Chart**

Shown in the upper left hand corner quadrant I, state meta data such as IP lease, current GPS location & time stamp can be harvested in the millisecond range to up 99 minutes. This data can be placed by a variety of publish-subscribe

type mechanisms (the heartbeat mechanism is a TCP/IP subnet publish subscribe mechanism) in local queues, file folders, or data stores for onward distribution by more modern & flexible protocols that usually rely on the heartbeat beacon mechanism. Transponder beacon sensor, mesh, telematic, & home awareness systems tech can move the data in the same millisecond range that the heartbeat protocol operates. This will enable faster than the current 30 second web page screen scrapes that exists because of data format differences between FAA & .mil systems. Shown in the lower left hand corner quadrant II, the heartbeat protocol is part of the TCP/IP stack. The heartbeat protocol / beacon (the term is used interchangeably) can query target devices on subnets for information stored on the device. The heartbeat mechanism gathers information that is assembled into heartbeat messages that are standards used by both network centric warfare template systems and National Emergency Numbering Association requirements for Public Safety Answering Points or PSAPs alike. The network meta / state data encapsulated in heartbeat messages change router/switch Management Information Bases or MIBS enabling units / platforms / devices / teams / organizations to be moved from network subnet to network subnet enabling network centric warfare style "maneuvering of the network" and "spontaneous integration".

Shown in the upper right hand quadrant III from top center is the International Telecommunications Union ITU its beacon symbol denoting a single, unified event / alert trigger for cross domain, cross community of interest COI instantiation / triggering of events and alerts via the OASIS ratified Common Alert Protocol CAP. The remainder of this quadrant depicts ingredients and baseline givens to make this possible. In the middle, a universal parsing agent replacing structured military messaging unique parsers is a key. Accessing common XML tags from national / international symbol set repositories is a given. Along the bottom of this quadrant is shown the current state of affairs between military organizations who use a variety of proprietary structured military message formats including formats that are hybrid XML header / structured military format body messages that are incompatible with first responder / commercial systems necessitating gateway systems that reduce reaction time, increase complexity and cost to all stakeholders. However, the common denominators between military and first responder systems is the heartbeat sub-protocol and heartbeat messages configuring state meta data enabling network reconfiguration.

Shown above lower right hand quadrant IV shows University of California's Ocean Store Sea Gull Beacon project's ability to increase / decrease the multicast radius coinciding with the increase or decrease of the DHS Homeland Security Advisory System (e.g., as magnitude of an earthquake increases or as a biological hazard vector spreads or the estimated blast / fall out radius....). South West Research Institute's SABRE is a sensor suite available to link low level tactical to strategic sensor enabled platforms. The Agile Delta / Tower Software represents the opportunity to replace proprietary military message formats such as the ground to air tactical situational awareness data links (TADLS or SADLs) with in use by the cabinet workflow /enterprise software suite enabling "chop chain" decisions based on actionable intelligence using every day tools.

The below shown diagram is the current Army Battle Command System / FBCB2 / Blue Force Tracker procedures. On the right, a commercialized, product/operating system/application neutral framework supporting the same functions to enable a global Situational Awareness Tone - SA Tone to smart phones & other mobile devices is shown. The heartbeat protocol as a low level data harvester gathers network configuration data (e.g., current IP lease, multicast group participation, state information such as moment greater than 50 meters, at halt, off line, or straggler…) that is gathered and forwarded by any newer, more efficient products or systems. Once multicast subscription group (s) state data is consolidated, data is consolidated by the tactical equivalent of the corporate system administrator or the S-6 in military terms.

The Tactical Internet Management System or TIMS is used to configure router management information bases (MIBS) and associated multicast entries describing the grouping of organizations (units) for missions (Unit Task Order). The S-6 / tactical system administrator then broadcasts the updated network configuration data in the form of (K00.99 Variable Message Format) heartbeat messages to higher, lower and adjacent organizations refreshing router/switch unicast / multicast subscriptions. On the military side of this procedural method, situational awareness data subscriptions are updated and units tether and un-tether to network nodes as they maneuver. A similar process occurs on the commercial side of this methodology as cell phone / smart phone / wireless laptop users tether and un-tether to cell tower nodes – differently i.e., different heartbeat protocol data collection-distribution rates and different heartbeat XML message schema structures). Heartbeat e9-1-1 involves the commercialization of network centric warfare message structures / documents / schemas into Emergency E9-1-1 cell phones and smart phones E9-1-1 Public Safety Answering Points – PSAPs emulation.

The Heartbeat Beacon involves commercialization of military proprietary tools such as the Tactical Internet Management System (TIMS) that produces the UTO – Unit Task Order. The UTO is a message template that

military situational awareness applications FBCB2 and Blue Force Tracking) apply. The Unit Task Order is a hierarchical depiction of unit structure showing how units are organized for operations similar to corporate wiring diagrams. UTO distribution is enabled by the use of TCP/IP's heartbeat mechanisms in terms of the heartbeat protocol's send to, get from and timer / data harvest trigger. Gathering network (re) configuration data used to update tactical / corporate organization / first responder's multicast subscription information based on unit / organizational mission posture change is key Heartbeat e9-1-1 methodology. The commercial equivalent of the military proprietary UTO Tool composes heartbeat protocol gathered network (re) configuration data as a XML EDXL-DE formatted schema with military DDMS data as embedded islands or child schemas. Commercial equivalent UTO tools will exchange network reconfiguration messages with military counterparts. Tool functionality includes updates to Multi-Cast Group (MCG) subscription data and Management Information Base (MIB). The UTO is part of the military TIMS (Tactical Internet Management System).

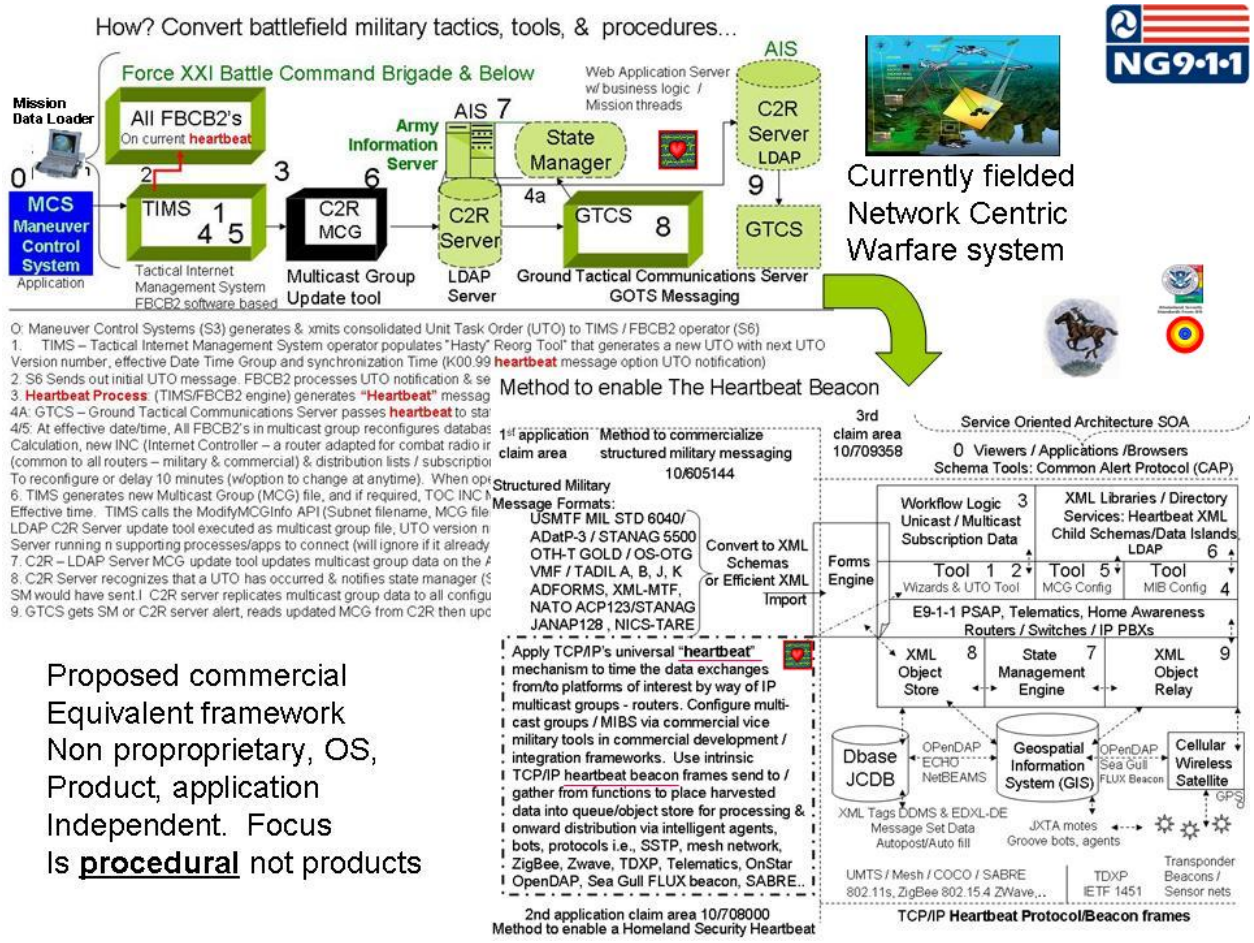


**Figure 3: .mil to .com conversion**

Situational awareness propagation systems apply workflow logic stored in APIs that are instantiated by scripts, defined by filters as implemented and broadcast by unicast / multicast IP groups supported by router/switches. The nearly universal heartbeat protocol as a low level data harvester, publish – subscribe & timing mechanism (2nd Claim Area) harvests & places network configuration data in files, queues, & object stores. Structured military messaging military unique field unit identifiers & field unit reference numbers (e.g., the time honored but now inflexible "FFIRNs and FUDs" & "DFI, DUI's") once converted to equivalent XML tags in Common Alert Protocol CAP) child schemas / embedded data islands format (1st Claim Area), will allow nearly any commercial forms engine with an XML parser to parse / process them for delivery by any more advanced sensor

/ data transport mechanism (e.g., Microsoft's Groove or Biztalk or ZigBee or TXDP… etc) providing forward and backwards interoperability & standardization for both the military and commercial systems.

The Heartbeat Beacon addresses data exchange gaps by stipulating CAP instantiated data exchanges for military, first responder, and commercial stake holder domains by standardizing data exchange formats, symbol sets, event refresh rates enabling direct collaboration with military telemetry systems using commercial products. Multicast radius will be adjustable e.g., increase / decrease with audible tones based on business logic / military mission thread logic according to threshold rules visually displayed as concentric color band expansion / collapse based on DHS five level color / audible advisory schemes. Alert, evacuation, alternate routing of transportation assets, medical triage will then are adjustable. Enabling an international Heartbeat Beacon for Homeland Security & Defense Interoperability & Synchronicity involves following a proven method / process and agreement on III building blocks / common denominators & 4 focus areas to standardize situational awareness (SA), event & alert data exchanges among N complex systems resulting in a global SA engine providing SA tone & SA as a service.