

# Cursor on Target: Research for a Sensor Network

Stevenson G<sup>1</sup>, Naiman M<sup>2</sup>, Valenta AL<sup>1</sup>, Boyd AD<sup>1</sup>

<sup>1</sup>College of Applied Health Sciences, University of Illinois at Chicago

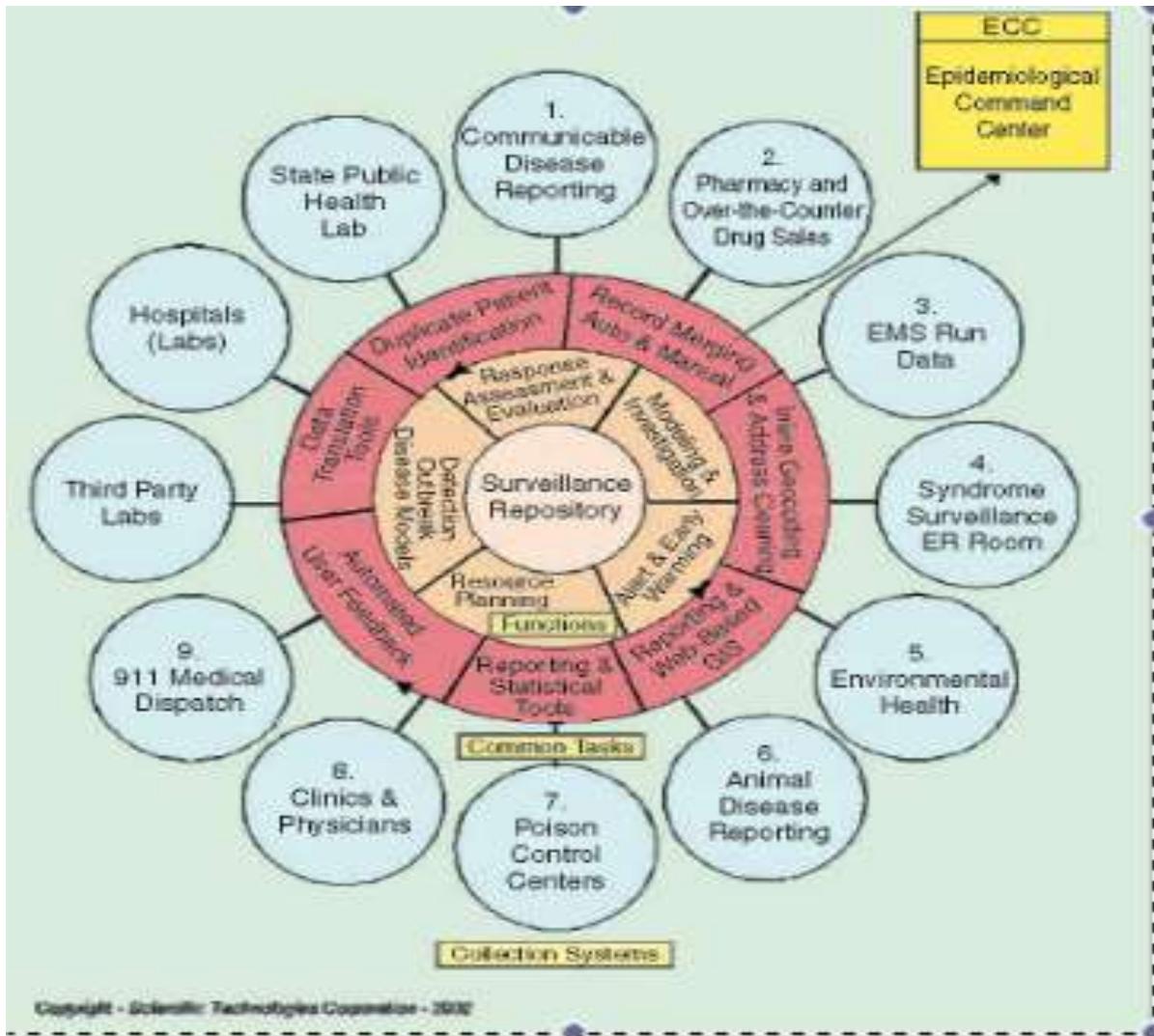
<sup>2</sup>Center for Advanced Design, Research And Exploration, University of Illinois at Chicago

## *Summary*

Terrorism, epidemics, natural, and man-made disasters have increased over the last decade, prompting ongoing evaluation and incremental rebuilding of the American public health system (Chan, Killeen, Griswold, & Lenert, 2004a; Yu, Brock, Mecozzi, Tran, & Kost, 2010). In February 2002, the Center for Disease Control (CDC) identified six focus areas to generate response capacities to bioterrorism and public emergencies. According to one focus area, information sharing and alert notifications between systems and public health agencies must be continuous and automatic (Popovich, Henderson, & Stinn, 2002). Advancements in technology set the stage for this uninterrupted data-sharing requirement to be met; for example, “smart devices” can digitally record and transmit information and text messages from remote disaster sites using wireless ad hoc networks. In this context, medical systems and personnel can provide enhanced patient support from the extraction point to the hospital, even when normal landline infrastructure has been damaged. However, care may be restricted due to the limited recognition of proprietary information and the distance between the transmitter and collector system. This article suggests that overcoming these limitations necessitates the adoption of interoperability by basic operations and illustrates how an Internet Protocol called Cursor-on-Target can facilitate communication between open source and propriety systems.

Interoperability is the exchange and processing of data between systems via a structured format and a common vocabulary. Disaster and emergency response support is comprised of three cyclical phases: 1) Pre-response analysis and dissemination; 2) Disaster and emergency support; 3) Post-deployment and re-initiation of the pre-response. In order to ensure rapid response and vigilance to any change in chemical, biological, natural, and/or nuclear conditions, unmanned sensors at all public health sites must send updated data around-the-clock to an Integrated Disease Surveillance System (IDSS) -- a public health data repository -- for analysis and dissemination (Popovich et al., 2002; see Figure 1). Information from multiple sources is required to sustain a disaster and emergency response capability. The sensor network must be supported by information feeds from all systems available to the combined public health organization. Studies have indicated that electronic automated disease reporting systems, which use extensible markup language (XML) format, are not only more efficient but also demonstrate the same accuracy as manual reporting procedures (Popovich, et al., 2002; Wurtz & Cameron, 2005).

To achieve interoperability, systems with a common output/interface can employ a multi-site licensed off-the-shelf translator purchased by a federal or state agency in order to decrease the overall cost of changing from one output format to XML. HIPAA (Health Information Portability and Accountability Act) electronic data interchange X12 (EDI X.12), and Health Level 7 (HL7) interface are commonly utilized for public health electronic disease information reporting (Popovich, et al., 2002; Wurtz & Cameron, 2005). Off-the-shelf software is also available to translate and map both HIPAA EDI X.12 and HL7 interfaces to extensible markup language. A foundation for the communications methodology is required to support safe data transportation, whether in the form of radio, Internet, or Wi-Fi. However, regulations, laws, policy, and protocol demand that the data be protected while in transit. Cursor-On-Target can provide that foundation using a machine language schema with the flexibility of a built in Internet document writer, beyond the existing patient centric interfaces mentioned above.



**Figure 1:** A vision for an integrated disease surveillance system (Popovich et al., 2002)

Cursor-on-Target (CoT) is an Internet Protocol and an XML based machine-to-machine schema that can be read and understood by any system, enabling proprietary and open source systems to communicate with each other. The schema can be used to transmit data from unmanned sensors to collector databases or be displayed on ArcGIS systems to indicate, for example, contamination expansion during a chemical disaster. During deployments, sensors can collect continuous data from a surrounding disaster area. The information can alert commanders to any chemical, biological, and/or natural contaminants. Therefore, commanders can be proactive in protecting their personnel instead of reactive once the symptoms emerge due to this enhanced situational awareness. CoT will allow personnel to use available communication signals to cross-communicate with each other and command, especially when the normal infrastructure is damaged or overloaded; all CoT transmissions are traced and displayed on routers. However, public health policies must advocate and provide credibility to the principle of interoperability to support data sharing, meet capacity goals, and enhance safety of the responders. This article presents an expansion on an earlier vision to implement interoperability across the entire public health system that remains compliant with HIPAA mandates. Interoperability must start with the full data sharing at the basic system level and continue through the command and control level during joint disaster response actions depending upon the agreements reached during interagency policy meetings.

## Background

Recent terrorism incidents coupled with natural and man-made disasters have forced the public health system into a perpetual capacity building mode(Harrison & Harrison, 2008; Popovich, et al., 2002; Yu, et al., 2010). Yet, advances in technology and changes in the role of information technology in disaster responses have resulted in a proliferation of sophisticated systems that aim to enhance the survivability of disaster patients (Chan, et al., 2004a; Harrison & Harrison, 2008; Popovich, et al., 2002). The American telecommunications system has undergone three upgrades in the last ten years and the wireless network protocol was upgraded to 802.11n in 2009. The new protocol contains provisions for advanced encryption standards, multiple-in multiple-out channels, and quality of service standards during transmissions. Internet protocol (IP) version 4 is upgrading to version 6, making it more attuned to mobile networks(Camp & Knightly, 2008; Chong Shen & Kwong, 2010; Choudhary & Sekelsky, 2010; Force, 2011; N. W. Group, 2006a, 2006b, 2007, 2009a, 2009b; Hiertz et al., 2008; Koskiahde, 2002; Nikander, Arkko, Aura, & Montenegro, 2003; Transformation, 2004; Villavicencio, Lu, Zhu, & Kota, 2007; Walke, Mangold, & Berlemann, 2006; Williams, Cansever, & Islam, 2006; Yang, 2005). Advancements in communications and computer systems technology have allowed medical systems to enhance patient recognition, medical record selection. Thus, remedial systems are no longer restricted to hospitals. Immediate remedial medical assistance can be identified at the point of an accident or disaster and given by a first responder until the patient is released from a recovery site(Chan, et al., 2004a).

Although technological advancements have supported medical system enhancements in the field, researchers have identified inter-connective errors in some of the remedial systems(Chan, et al.,

2004a). Although programs were tested and deemed operational under simulated disaster criteria in a closed system, these conditions do not reflect the real-world environment (Chan, et al., 2004a). Thus, any errors were identified as network-related oversights such as problems of coordination and real-time data acquisition. When more realistic situations or actual usage tests were performed, the systems experienced some connectivity failures, especially in cases where transmission point and receipt site were distant from one another and where transmission path was obscured. Consequently, the full disaster contingency plan was not activated. In real world disaster responses, public health personnel rely on multiple health agencies and medical responders for help with wounded patients. Like the general population, all such agencies utilize airwaves, cellular phones, and Wi-Fi. System overload eventually causes the communications systems to crash, as happened during Katrina and 9/11 (Harrison & Harrison, 2008; Popovich, et al., 2002). A communication methodology or platform that optimizes joint usage for more throughput of the same bandwidth (while minimizing the overall impact on the bandwidth) can address these challenges. For example, a rescue helicopter could act as a router for an Internet Protocol address message if the aircraft was closer than the next known router. Interoperability ensures that data in a common language or format flows smoothly through the system.

## **Interoperability**

Interoperability is “the ability of different systems to exchange information so that it can be processed meaningfully by all systems involved, e.g., between different software products or sub-systems elements, hardware devices, or multiple networks” (Hargrave, 2001). Challenges to interoperability have been studied from many perspectives, including health care, information technology, and military. It has been noted that some military systems do not have the capability to exchange information in a meaningful manner (Hatzipapafotiou & Kreisler, 2005; Hernandez, 2007; Suri et al., 2009; Transformation, 2004; White, 2001). As a result, NATO is encouraging enforcement of communication interoperability for any aircraft and communication system coming online (Kenyon, 2008). Interoperability would allow personnel and equipment to communicate with and through each other while cutting down on actual bandwidth use. All authorized command sites would have a full, consolidated functional picture that incorporates data from a range of participants in a disaster response, including first responders with an iPhone application providing air evacuation departure schedules. Interoperability would allow timely joint response to any situation while enhancing working communication control. The system must meet one criterion only: it must be communication interoperable with all other systems in the inventory. Concurrently, message routing and flow would be optimized vertically and horizontally within any singularly contained or mixed response group. The optimization is based on a common thread that exist between all the data and communication systems currently in use and any that will be allowed to be put into the inventory in the future. All systems must be able to converse with each other using the common machine language that the Extend Markup Language is based upon (Harold, 1999).

When speaking of communications between or within an interdisciplinary group like a disaster response team or even the public health system, interoperability must cover proprietary data, sensory, and communication systems. Interoperability, however, is only part of the answer to the communications problem. Policy must guide interoperability, control security and technology,

and the formatting and sharing of information. Further, interoperability must be regularly tested, as is the case for any form of health technology, and documented in accordance with applicable federal, state, and local laws, regulations, and policies. Without regular testing the systems may not work when needed.

## Policy

Federal, state, and local agencies need explicit intergovernmental roles and responsibilities around interoperability in public health policy. This policy should provide a method for putting interoperability into action, and provide guidelines or limitations on data sharing and group interaction. The guidelines should stipulate when data is available to outside agencies, the responsibility of each agency, and the chain of command during declared emergencies. Because disaster and bioterrorism scenarios are not stable and technological advancements occur rapidly, this policy must be flexible and be comprised of standards that can be adjusted to suit diverse and evolving emergencies (GAO, 2003). Finally, policy should implement guidelines for collecting “baseline” data from laboratory-based reporting systems, hospitals, and federal, state, and local health agencies during pre-disaster deployment phases. All agencies need to train with the available data before encountering it for the first time in the disaster.

## Translators

Protected Health Information (PHI) must be electronically transmitted during disasters, bioterrorism events, and public health emergencies. Patient information must be secured and transmitted to the receiving data sites, preferably in a format that will be recognized by installed applications. With the emergence of Regional Health Information Networks, data about the patients at a disaster site could be made available to responders for triage purposes. To access such information, a data translation tool for HL7 and EDI X12 are necessary. EDI X12 can be translated using java or multiple other off-the-shelf translators that convert all known X12 HIPAA formats to extensible markup language (XML) format. These translators support EDI for HIPAA 5010 and International Classification for Disease -10. HL7 interfaces can use default encoding in a delimiter-based format called HL7 version 2.2 or 2.3 (International, 2012). Additionally, Level 7 can also use a XML format, and some entities have been migrating to the XML format.

However, not all data relevant to a disaster response will contain PHI. For example, Panackal et al (Panackal et al., 2002) and Wurtz and Cameron (Wurtz & Cameron, 2005) indicate that electronic laboratory reporting (ELR) for infectious diseases is faster, more complete, and just as accurate as reporting done by hand. Because the ELR uses HL7 format and an Oracle database, de-identified data can be easily translated to an XML format and displayed on a viewer for tracking purposes. ELR is growing rapidly. An Arc-GIS interface has already been built for the U.S. Air Force (Odom, 2008) and there are interfaces to global positioning systems (GPS), Google Earth, and Falcon View. These display systems utilize the XML tracking mechanism and the input from GPS to place moving assets such as aircraft, meteorological cloud boundaries, and personnel accurately (General Dynamics, 2011).

## Cursor-on-Target

The proposed foundation for transmission interoperability is a machine-to-machine based schema called Curser-on-Target (CoT) built by the MITRE Corporation and the Air Force. CoT is a methodology that reduces interoperability problems while enhancing information technology using basic machine capabilities. “Cursor-on-Target” was coined when an Air Force general called for integration of the multiple systems under his control. “The sum of all wisdom is a cursor over the target,” his catchphrase, became the namesake for CoT. The schema transmits a target’s “what (type), where (coordinates), and when (time)” without risk of human error or delay. CoT is transport agnostic, as the appropriate choice of transport depends on the data that is being moved (e.g., file transfer protocol (FTP), transfer control protocol (TCP), hypertext transfer protocol (http), and so on) (C. O. T. U. Group, 2010).

The format does not prevent developers from using fourth-generation languages to interact with proprietary systems as translators or information carriers to update and share cross-platforms. CoT can update one or many sites at once depending on the parameters set within the schema. XML is open source, and easy to read and write, and the language's tag properties enhance its versatility. One or many entity details can be transported in a single CoT message under a singular identification, and each detail’s identifying tag marks it as a new detail record. This ability, together with the message’s normal small bandwidth use, minimizes network usage.

The CoT router’s user guide suggests that the schema is defined in “Event.xsd,” and is registered in the Defense Information Systems Agency (DISA) Department of Defense (DoD) XML registry (Kristan, Hamalainen, Robbins, & Newell, 2009). The schema is available at MITRE’s website: <http://cot.mitre.org>. The schema is terse (concise) and effectively describes “what, when, and where.” An example of the schema is expressed in Figure 2.

```
<?xml version='1.0' standalone='yes'?>
<event version="2.0"
  uid="J-01334"
  type="a-h-A-M-F-U-M"
  time="2005-04-05T11:43:38.07Z"
  start="2005-04-05T11:43:38.07Z"
  stale="2005-04-05T11:45:38.07Z" >
  <detail>
  </detail>
  <point lat="30.0090027" lon="-85.9578735" ce="45.3"
    hae="-42.6" le="99.5" />
</event>
```

**Figure 2:** Basic CoT XML Message (Kristan et al., 2009)

The schema has twelve mandatory attributes and can hold multiple sub-schemas through the manipulation of other XML tags (C. O. T. U. Group, 2010). As shown in Figure 2, CoT utilizes three main types of tags. The first tag is the event tag and provides information with unique identification (UID): hierarchical data on the object of interest (type); time the message was generated (time); time the event became of interest (start); time the event is no longer of interest (stale). The “a” in the type line indicates the “atoms branch of the tree” defining detailed types given in Military Standards 2525B specification. Military Standards 2525B is the document that gives the symbolic representation and corresponding unique identifier of assets and threats and guarantees quick interpretation by anyone who is familiar with the specification. The second tag is the point tag, which gives the geo-localized position and elevation of the item of interest. Lastly, the detail tag enables users to transmit data and/or records to applications or systems using the structured XML format. XML schema accepts extensible style language tags that generate reports, structure Web screens, and change reports based on input based on data received from unmanned sensors (C. O. T. U. Group, 2010; Kristan, et al., 2009). Given the wide range of unmanned sensors being developed, the flexibility of this standard and the ability to integrate with GIS systems provides a robust interface beyond the existing capabilities.

These capabilities enable and strengthen communication to and between proprietary systems. As long as there is a network connection, CoT can expand the combined situational knowledge of a disaster area and data transmittal distance by sharing broadcast power and bandwidth. At the Third Annual Cursor-on-Target (CoT) Users Group conference convened in 2011, the group demonstrated fifteen disparate systems continuously transmitting and receiving messages from each other. While overall routing was accomplished through a main router, multiple routers directed the message through various vendor system sessions as a test of connectivity.

## Security

Security measures are considered more reliable when the measures are layered. Thus, if one layer fails, the subsequent layers can intercede and prevail where the preceding layer failed (Tipton, 2010). Security for Cursor-on-Target is controlled through the basic schema given in the user’s guide (Kristan, et al., 2009) as shown in Figure 2. The transmission must meet a valid format, but it also must include an authorized UID, symbolic type code, latitude, and longitude or the transmission will be ignored. The UID must be registered with the controlling Internet Protocol controller before the UID will be recognized on the channel, which is controlled via IP v6. Internet Protocol version 6 is more secure than version 4 and uses a more sophisticated risk adaptive access control and dynamic security response to changing operational situation (Choudhary & Sekelsky, 2010).

The XML format allows encryption within the format tags (Harold, 1999). Thus, when used in conjunction with the flexibility built into the user’s guide and the XML structure, encryption provides CoT transmission a third and fourth layer of security.

## Discussion

In the last two decades, there have been three million deaths due to terrorist attacks, floods, earthquakes, and disease outbreak. Health care shoulders a tremendous degradation in its emergency medical response ability amid personnel and budget reductions. Yet, crisis response cannot be reduced as disasters require enhanced mobility tasking. Secondary response capability to an active disaster-recovery area is decreased by infrastructure damage at the event site. A constant but undetermined drain on the medical supply stockpile used to replenish remote site(s) continues. Depending on the level of infrastructure damage at the disaster site, central control may not be aware of the situation on the ground (Chan, et al., 2004a; Harrison & Harrison, 2008; Popovich, et al., 2002). Field commanders make quick decisions, sometimes basing them on an incomplete tactical situational picture. Enhanced interoperability complemented by the communication power of CoT can provide commanders the comprehensive picture, vertically and horizontally, they require to make informed decisions.

The vertical communication flow between responders and the horizontal flow to site commanders provides an effective chain of command for efficient data and communication channels. Interoperability must be used in conjunction with an on-site command structure. As inability to communicate effectively leads to lost lives (Panackal, et al., 2002), planning and cooperation can and should address barriers to communication and interoperability.

Harrison and Harrison (2008) advocate a disaster response view based on regional, national, and international efforts to coordinate an effective reaction methodology that provides for local, state, and federal programs established on technological architecture. This architecture would be the foundation for communications, management, and administrative control and interoperability. Their proposal aims to ensure optimal use of medical records, geographic information systems and tracking systems and, most importantly, to generate improved medical response capabilities. Chan et al. (Chan, et al., 2004a) suggest that overcoming potential infrastructure damage by way of layered communication systems is a major disaster response challenge. IP-based Cursor-on-Target is flexible and able to multi-cast information collected from satellite, landline, mobile, and Wi-Fi channels. Such multi-cast capability enables coordinated medical responses by broadcasting alerts or request messages to numerous on and off-site control centers (William O Jenkins, 2003).

The US Joint Command tested the capabilities of CoT XML during an exercise that combined the competencies of three distinctive systems to control intelligence, surveillance, and reconnaissance assets. Typically, information from one system is displayed only on its individual screen. To address the lack of communication between systems, four small translation programs -- one per system -- transformed the data to CoT's XML format. Three systems updated a fourth, which in turn updated all systems, allowing information from all four systems to appear on all screens (including a laptop). The Joint Command is scaling up their use of CoT XML to include radio transmissions and chat protocols (Lawlor, 2005).

Public health systems should leverage the capabilities of CoT (i.e., using XML to update separate, but disparate proprietary systems) to meet the CDC's capacity goal for data sharing.

Data sharing and interoperability transcend national borders and flow intrinsically with the medical, public, and military health personnel whether they are deployed to third world areas or within US borders. Interoperability, for example, could have prevented the overloaded communication systems and miscommunicated verbal orders that caused critical patients at the World Trade Center (WTC) in 2001 to be routed to non-critical care hospitals (Chan, Killeen, Griswold, & Lenert, 2004b). CoT can link the IDSS with the remote chemical sensors and a geographic information system during pre- and post- deployment periods or allow sensors to be placed strategically to provide data during deployments. Furthermore, CoT has a stale time to indicate when the sensor information is no longer valid. Finally, CoT ensures data security by encrypting PHI. CoT uses codes to designate the “what” of the message, and the PHI could be encapsulated within the detail sub-schema. The sub-schema can be encrypted within the detail tag format; thus, the transmission will meet the requirements of HIPAA. The ability of CoT to transmit the geo-position of a patient or track the movement of the boundary of chemicals through tracing when used with ArcGIS or other applications can visually alert responders to impending danger, which would dramatically expand the current capabilities of any health care data interchange

Overseas joint humanitarian relief responses have been hampered by the lack of evidence-based medical assistance and care. Healthcare reporting during and after any disaster, bioterrorism, or emergency response action necessary for future evidence-based medical procedures were incomplete due to minimal communications. Information is manually captured then lost or never transferred to a database for analysis. Most health operations following the initial rescue entail delivery of medical assistance to the injured and efforts to contain or slow the spread of contagions due to unsanitary conditions and close living quarters. Evidence-based information is critical to lower the projected morbidity rate during initial triage stages of a disaster (Banatvala & Zwi, 2000; Brattberg & Sundelius, 2011; Fernando & Hilhorst, 2006; Jr, Mayer, Mason, Jr, & Mahoney, 1985; Posen, 1996; Queen & Pugh, 1992). The reports and information from teams on the front lines provide data to maximize humanitarian evidence-based care while minimizing diseases due to destroyed infrastructure and diminished living conditions. These conditions continue as the responders leave the affected area after an initial ninety or hundred-eighty day window without repairing the underlying communication infrastructure. For example, an ineffective communication infrastructure in Haiti still degrades the point-of-care testing and evidence-based care giving and data gathering in some urban and most rural areas. Thus, diseases and morbidity rates continue to climb and patients are being tracked via mobile phones during the disaster recovery and rebuild period (Bengtsson, Xin, Thorson, Garfield, & von Schreeb, 2011). CoT or another XML based communication schema that enhances interoperability and is approved for release to third world countries could increase the speed and quality of evidence-based care and data exchange during and after disasters. It would also ensure the quality of research data for future evidence-based procedures while increasing the quality of health in the host community.

CoT allows captured data to be manipulated using extensible style language (XSL) (Harold, 1999). XSL can be used to show visual ranges from sensor output in print format. XSL is simple to use, machine language based, and can be used in a hierarchical (class) manner. Reports can be formatted in any way that is needed and delivered straight to a printer in a graphical

presentation or to a display in text form. Of course, the data can be formatted using XML or XSL and imported directly into a database for analysis at a later date with current needs being met by mobile applications.

The versatility of the sub-schemas allows on-the-go modifications with minimal problems and downtime. It also has the add benefit of multicasting to different commands and allowing all levels of personnel to converse in a secure and quick manner. These latter components are great assets if the health units operate with other Task Forces that use CoT or another XML interoperable schema; thus, the cross communication between forces and vertical command and control communication lines is increased. Data can be sent to collectors for analysis to assist public and military health personnel with building an evidence-based response. The transport schema assists in providing cross-communications while public and military health personnel treat the affected population for injuries and diseases prevalent in overcrowded populated areas under great stress.

## **Limitations**

CoT must be built for each interface with a device and tags delimit fields with the field for comments being set by the remark tags. The CoT router routes all messages from one host to another host and holds all the pertinent rules and destination addresses. CoT must contain twelve schema tags and cannot deviate from that structure. The schema requires an initial setup of the hierarchy and privileges to utilize the structure. However, these minor stipulations will open the door to interoperability. The XML format and tag usage provides flexibility to each agency and or/unit to determine how they want the output to look at the final destination while meeting the mandated interoperability requirements for data sharing and bandwidth transmission capabilities.

## **Conclusion**

Economically, CoT is the most efficient and effective methodology to join old and new technology with policy and strategy to gain interoperability. It can dampen technological problems while enhancing communications during a disaster response. CoT's ability to interact with any cross-platform system as it did during the Joint Command exercise keeps personnel "in the loop" where they can be proactive instead of reactive (Lawlor, 2005). It also provides quicker and easier interagency communication, when public health responders are deployed with military health units. As "smart devices" become ubiquitous, CoT enables health or other personnel to accurately position themselves via maps or directives displayed on an iPhone, preempting errors that often arise in utilizing radio for such communication, for example. Of course, data can be formatted using XML or XSL and be imported directly into databases for analysis at a later date with current needs being met by mobile applications.

For the American global disaster response policy to work at maximum capability, the interdiction should be based on rapid deployment of evidence-base care to displaced inhabitants together with evacuation of those listed as missing (Brattberg & Sundelius, 2011; Chan, et al., 2004a; Fernando & Hilhorst, 2006; Jr, et al., 1985; Posen, 1996; Queen & Pugh, 1992; Yu, et al., 2010).

Evidence-based medicine requires an available comprehensive database that will provide and accept data from on-site triage facilities. Physicians should be able to share data with and train in-county public health agencies and clinicians in an effort to stem long-term morbidities and disease outbreaks. A network-centric communication foundation based on CoT would provide the capability for a joint global civilian/military public and medical health task force to share medical information collection equipment and data rapidly and securely with each other (Popovich, et al., 2002; Shulstad, 2011; Transformation, 2004). CoT would also allow the medical task force to converse and share information with the American military forces sent to secure the area and patch information back to the United States via satellite connections. Homeland Security, Justice Department, Military, and members of the medical and public health field, to include the CDC, are already calling for interoperability and rapid disaster response capabilities that are built on sharing data before, during, and after a disaster (Banatvala & Zwi, 2000; Bengtsson, et al., 2011; Brattberg & Sundelius, 2011; Brown, Griswold, & Lenert, 2005; Chan, et al., 2004a; Fernando & Hilhorst, 2006; GAO, 2003; Gurss, 2011; Harrison & Harrison, 2008; Jr, et al., 1985; Kenyon, 2008; Lawlor, 2005; Lenert, Palmer, Chan, & Rao, 2005; Popovich, et al., 2002; Programs, 2005; Sharp, Burkle, Vaughn, Chotani, & Brennan, 2002; Terry, 2012; William O Jenkins, 2003; Yu, et al., 2010).

However, Cursor-on-Target entails some initial work to build the hierarchy. Currently, Military Standard 2525B does not contain codes related to health as the standards relate to symbolic codes for war fighting vehicles and structures (Fletcher, Arnold, & Cockshell, 2011) . However, the CoT Users Group is glad to assist with setting up the necessary codes. Building the system hierarchy should be done in tandem with policy decisions as the code will affect everyone, unless there will be two hierarchies, one each for public and military health. Two codes would defeat the purpose of interoperability and slow the process of communicating and saving lives during a joint disaster operation. All organizations have found it is best to cut costs and share data while maintaining the cutting edge readiness necessary to protect people and property from natural or man-made disasters, terrorism, and emergencies. The Justice Department and Homeland Security are building their shared foundation using XML (Programs, 2005). CoT can help ensure that human life is protected proactively instead of reactively.

## **Corresponding Author**

Greer Stevenson  
Clinical Assistant Professor  
College of Applied Health Sciences  
University of Illinois at Chicago  
Email: gsteve1@uic.edu

## References

- [1] Banatvala, N., & Zwi, A. B. (2000). Conflict And Health: Public Health And Humanitarian Interventions: Developing The Evidence Base. *BMJ: British Medical Journal*, 321(7253), 101-105.
- [2] Bengtsson, L., Xin, L., Thorson, A., Garfield, R., & von Schreeb, J. (2011). Improved Response to Disasters and Outbreaks by Tracking Population Movements with Mobile Phone Network Data: A Post-Earthquake Geospatial Study in Haiti. [Article]. *PLoS Medicine*, 8(8), 1-9.
- [3] Brattberg, E., & Sundelius, B. (2011). Mobilizing for International Disaster Relief: Comparing U.S. and EU Approaches to the 2010 Haiti Earthquake. *Journal of Homeland Security and Emergency Management*, 8(1, Article 24).
- [4] Brown, S., Griswold, W., & Lenert, L. A. (2005). A Web-Services Architecture Designed for Intermittent Connectivity to Support Medical Response to Disasters. *AMIA Symposium Proceedings*, 1.
- [5] Camp, J., & Knightly, E. (2008). The IEEE 802.11s Extended Service Set Mesh Networking Standard. *Communications Magazine, IEEE*, 46(8), 120-126.
- [6] Chan, T. C., Killeen, J., Griswold, W., & Lenert, L. (2004a). Information Technology and Emergency Medical Care during Disasters. *ACAD EMERG MED*, 11(11), 8.
- [7] Chan, T. C., Killeen, J., Griswold, W., & Lenert, L. (2004b). Information Technology and Emergency Medical Care during Disasters. *ACAD EMERG MED*, 11(11), 1229-1236.
- [8] Chong Shen, W. D., Robert Atkinson, & Kwong, K. H. (2010). Policy Based Mobility & Flow Management for IPv6 Heterogeneous Wireless Networks. *Wireless Pers Commun.* doi:10.1007/s11277-010-0056-y
- [9] Choudhary, A. R., & Sekelsky, A. (2010, 8-10 Nov. 2010). *Securing IPv6 network infrastructure: A new security model*. Paper presented at the Technologies for Homeland Security (HST), 2010 IEEE International Conference on.
- [10] Fernando, U., & Hilhorst, D. (2006). Everyday Practices of Humanitarian Aid: Tsunami Response in Sri Lanka. *Development in Practice*, 16(3/4), 292-302.
- [11] Fletcher, K., Arnold, A., & Cockshell, S. (2011). Detection of Common Warfighting Symbolology (MIL-STD-2525) Air Symbols. *Maritime Operations Division Defense Science and Technology Organisation, DSTO-TR-2604*.
- [12] Force, I. E. T. (2011). Mobility Support in IPv6, *RFC6275* (Vol. 6275).
- [13] GAO. (2003). *Homeland Security - Challenges in Achieving Interoperable Communications for First Responders*. Retrieved from <http://www.gao.gov/new.items/d04231t.pdf>.
- [14] General Dynamics. (2011). Open Net-Centric Interfaces. *C4 Systems* Retrieved February 29, 2012, 2012, from <http://www.fortresstech.com/Technology-Article/open-interfaces.html>
- [15] Group, C. O. T. U. (2010). Cursor on Target FAQ.
- [16] Group, N. W. (2006a). Authentication Protocol for Mobile IPv6, *RFC4285* (Vol. RFC4285).
- [17] Group, N. W. (2006b). Experimental Values in IPv4, IPv6, ICMPv4, ICMPv6, UDP, and TCP Headers, *RFC4727* (Vol. RFC4727).
- [18] Group, N. W. (2007). Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture, *RFC4877* (Vol. RFC4877).

- [19] Group, N. W. (2009a). Authentication, Authorization, and Accounting (AAA) Goals for Mobile IPv6, *RFC5637* (Vol. RFC5637).
- [20] Group, N. W. (2009b). Mobile IPv6 Fast Handovers, *RFC5568* (Vol. RFC5568).
- [21] Gurs, R. M. (2011). Calling All Cars? Be Sure To Use LTE On 700 MHz. *The Law of Communications*. Retrieved from <http://www.commlawblog.com/2011/02/articles/internet/calling-all-cars-be-sure-to-use-lte-on-700-mhz/>
- [22] Hargrave, F. (2001). Wiley-IEEE Press.
- [23] Harold, E. R. (1999). *XML Bible*. Foster City, CA: IDG Books Worldwide, Inc.
- [24] Harrison, J. P., & Harrison, R. A. (2008). Role of Information Technology in Disaster Medical Response. *The Health Care Manager*, 27(4), 307 - 313.
- [25] Hatzipapafotiou, D., & Kreisler, S. (2005, 17-20 Oct. 2005). *Test and demonstration environment for net-centric operations*. Paper presented at the Military Communications Conference, 2005. MILCOM 2005. IEEE.
- [26] Hernandez, D. (2007, 29-31 Oct. 2007). *Airborne Solutions for True Net-Centric Connectivity at the Tactical Edge*. Paper presented at the Military Communications Conference, 2007. MILCOM 2007. IEEE.
- [27] Hiertz, G. R., Zang, Y., Max, S., Junge, T., Weiss, E., & Wolz, B. (2008). IEEE 802.11s: WLAN mesh standardization and high performance extensions. *Network, IEEE*, 22(3), 12-19.
- [28] International, H. L. S. (2012). HL7 International. Retrieved March 15, 2012, 2012, from <http://www.hl7.org/index.cfm?ref=nav>
- [29] Jr, E. N. B., Mayer, W. N., Mason, J. O., Jr, D. E. B., & Mahoney, L. E. (1985). Designing a National Disaster Medical System. *Public Health Reports (1974-)*, 100(5), 455-461.
- [30] Kenyon, H. S. (Producer). (2008, 2/1/2012) Interoperability Key to Multinational Operations. *Signal Online*. retrieved from [http://www.afcea.org/signal/articles/templates/SIGNAL\\_Article\\_Template.asp?articleid=1686&zoneid=47](http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=1686&zoneid=47)
- [31] Koskiahde, T. (2002). MIPv6. Tampere University of Technology.
- [32] Kristan, M. J., Hamalainen, J. T., Robbins, D. P., & Newell, P. (2009). Cursor-on Target Message Router User's Guide. In Mitre (Ed.), *Mitre Product* (Vol. MP090284, pp. 1-34). Bedford, Massachusetts: Mitre Products.
- [33] Lawlor, M. (Producer). (2005) Communications Capabilities Connect. *Signal Online*. retrieved from <http://www.afcea.org/signal/articles/anmviewer.asp?a=735>
- [34] Lenert, L. A., Palmer, D. A., Chan, T. C., & Rao, R. (2005). An Intelligent 802.11 Triage Tag For Medical Response to Disasters. *AMIA Symposium Proceedings*, 5.
- [35] Nikander, P., Arkko, J., Aura, T., & Montenegro, G. (2003). Mobile IP Version 6 (MIPv6) Route Optimization Security Design. *IEEE VEHICULAR TECHNOLOGY CONFERENCE*, 3(Conf 58), 2004-2008.
- [36] Odom, J. (2008). Integration of FalconView and ArcGIS. Retrieved February 11, 2012, from <http://giscoder.blogspot.com/2008/03/integration-of-falconview-and-arcgis.html>
- [37] Panackal, A. A., M'Ikanatha N, M., Tsui, F. C., McMahan, J., Wagner, M. M., Dixon, B. W., et al. (2002). Automatic electronic laboratory-based reporting of notifiable infectious diseases at a large health system. *Emerg Infect Dis*, 8(7), 685-691.

- [38] Popovich, M., Henderson, J., & Stinn, J. (2002). Information Technology in the Age of Emergency Public Health Response. *IEEE Engineering in Medicine and Biology, September/October*, 48 - 55.
- [39] Posen, B. R. (1996). Military Responses to Refugee Disasters. *International Security, 21*(1), 72-111.
- [40] Programs, O. o. J. (2005). Information Technology Initiatives. *The Information Sharing Resource for the Justice and Public Safety Communities* Retrieved March 30, 2012, 2012, from <http://it.ojp.gov/jxdm/>
- [41] Queen, K. B., & Pugh, E. J. (1992). Medical response to disasters overseas. [Comment Letter]. *BMJ, 304*(6836), 1249.
- [42] Sharp, T. W., Burkle, F. M., Jr., Vaughn, A. F., Chotani, R., & Brennan, R. J. (2002). Challenges and Opportunities for Humanitarian Relief in Afghanistan. *Clinical Infectious Diseases, 34*(ArticleType: research-article / Issue Title: Supplement 5. Afghanistan: Health Challenges Facing Deployed Troops, Peacekeepers, and Refugees / Full publication date: Jun. 15, 2002 / Copyright © 2002 Oxford University Press), S215-S228.
- [43] Shulstad, R. A. (2011). Cursor on Target. *Air & Space Power Journal*(Winter 2011), 19 - 28.
- [44] Suri, N., Benvegna, E., Tortonesi, M., Stefanelli, C., Kovach, J., & Hanna, J. (2009). Communications middleware for tactical environments: Observations, experiences, and lessons learned. *Communications Magazine, IEEE, 47*(10), 56-63.
- [45] Terry, K. (2012). EHR Certification Proposal Stresses Interoperability. *InformationWeek Healthcare*. Retrieved from <http://www.informationweek.com/news/healthcare/EMR/232601824>
- [46] Tipton, H. F. (Ed.). (2010). *Official (ISC)2 Guide to The CISSP CBK* (2 ed.). Boca Raton: CRC Press.
- [47] Transformation, D. F. (2004). Network-Centric Warfare. In O. o. t. S. o. Defense (Ed.), *Director, Force Transformation*. Washington D.C. : Department of Defense.
- [48] Villavicencio, O., Lu, K., Zhu, H., & Kota, S. (2007, 29-31 Oct. 2007). *Performance of IEEE 802.11n in Multi-Channel Multi-Radio Wireless Ad Hoc Network*. Paper presented at the Military Communications Conference, 2007. MILCOM 2007. IEEE.
- [49] Walke, B. H., Mangold, S., & Berlemann, L. (2006). *IEEE 802 Wireless Systems*. Hoboken: Wiley.
- [50] White, B. E. (2001). *Communications for Network-Centric Operations: Creating the Information Force*. Paper presented at the Military Communications Conference, 2001.
- [51] William O Jenkins, J. (2003). *Homeland Security - Challenges in Achieving Interoperable Communications for First Responders*. Retrieved from <http://www.gao.gov/new.items/d04231t.pdf>.
- [52] Williams, C., Cansever, D., & Islam, J. (2006, 23-25 Oct. 2006). *A Portable Mobile IPv6 Architecture for Net-Centric Warfare*. Paper presented at the Military Communications Conference, 2006. MILCOM 2006. IEEE.
- [53] Wurtz, R., & Cameron, B. J. (2005). Electronic laboratory reporting for the infectious diseases physician and clinical microbiologist. *Clin Infect Dis, 40*(11), 1638-1643.
- [54] Yang, X. (2005). Performance analysis of priority schemes for IEEE 802.11 and IEEE 802.11e wireless LANs. *Wireless Communications, IEEE Transactions on, 4*(4), 1506-1515.
- [55] Yu, J. N., Brock, T. K., Mecozzi, D. M., Tran, N. K., & Kost, G. J. (2010). Future connectivity for disaster and emergency point of care. *Point Care Point of Care, 9*(4), 185-192.