APPLYING SEMANTIC TECHNOLOGIES, POLICY FRAMEWORKS, AND DISSEMINATION SERVICES TO SUPPORT INFORMATION GATHERING AND SHARING

Matthew Johnson, Larry Bunch, Jeffrey M. Bradshaw, Pau J. Feltovich,
James Lott, NIranjan Suri, Maggie Breedy
Florida Institute for Human and Machine Cognition (IHMC)
Pensacola, Florida

Eric Heilman
US Army Research Laboratory
Tactical Information Fusion Branch

DRAFT: 29 March 2010

The most crucial factor limiting US military dominance today is information. In the end it comes down to what General Chiarelli referred to as the goal of the network: "Right Information – Right Place – Right Time" [1]. Though this requirement is often couched as an information sharing issue, the challenge of gathering the right information in a timely manner is often equally at the root of the problem. Information gathering in today's counterinsurgency environment differs from information gathering in a conventional war. Major General Flynn's paper [2] on fixing intelligence suggests that today's conflicts are different in both *what* needs to be gathered and *who* needs to gather it. Flynn suggests that we need to gather information, not just about the enemy, but also about the local area, structures, capabilities, organizations, people and events (ASCOPE). He also suggests that the Soldier on the ground is the best source for this information; a sentiment echoed by General Chiarelli [1]. All of this, taken together, means that the Soldiers bear a double burden in a counterinsurgency because they are both the most important *consumers* and *suppliers* of information. It also means that collection is now occurring at the tactical edge of the Army and frequently "outside the wire" in remote and computing-resource-poor areas. Realizing the importance of addressing these critical needs, an increasing number of military applications are being targeted toward information gathering and sharing. For practical reasons, these applications are being designed to work on portable devices—not only laptops, but also tablet computers and smartphones. However, despite these advances in new applications and devices, the challenges of effective information gathering and sharing will never be solved unless more attention is paid to the less glamorous but equally essential problem of making the information itself and the networks that carry it "smarter." In this white paper, we will show how a combination of semantic technologies, advanced policy frameworks, and dissemination services can help support the information needs of a soldier as a consumer and supplier who is operating in a peer-to-peer manner with a variety of people

that have different interests and access rights in an environment with low-bandwidth and intermittent network connectivity[1].

BRIEF OVERVIEW OF THE TECHNOLOGIES

SEMANTIC KNOWLEDGE REPRESENTATIONS

Semantics is about meaning. People are very good at assessing the context of a statement and inferring meaning. Machines are not. A vast amount of information today is digital and we are always looking for new ways to automate solutions for information challenges. Often this is done by using human assessment to rigidly apply an implicit informational relationship. Data without any labeling is fairly useless. Our recent efforts [3] have been to associate formal semantic knowledge representations with the data to allow for more flexible and complex associations to be made automatically. The simplest labeling is categorization. Semantics, if properly used provides not only a description of what this piece of data is, but also the contexts in which the data is actionable. For example, simple categories can be used to determine what to do with the data. Identifying PUBLIC and PRIVATE data as such is nice, but understanding what that means for dissemination and being able to control and manage that dynamically is what our services are all about. Categories are just one simple application of semantic labels. However, semantic knowledge representations can be much more complex to include a variety of relationships that add rich context, such as hierarchical relationships, composition, sub-classing and many other types of relationships. Semantic technologies are used to describe the properties and features of information and how these relate to mission context; thus, they are capable of providing the best set of available tactical information to the soldier in the field. A simple way to think about the issue is that semantics allows for interpretive automation. A good infrastructure of services needs to make use of semantics to provide opportunities in a dynamic and flexible way.

KAOS POLICY SERVICES

KAoS policy services [4] can dynamically manage information flow and help address issues associated with the lateral and potentially open sharing environments. It is used to managed access (who can and cannot get the data), bandwidth (what can be passed) and priority (what is most important). KAoS uses sets of policies to express and enforce these constraints. Policies

[1] Research was sponsored by the Army Research Laboratory and was accomplished under Cooperative Agreement Number W911NF-08-2-0049. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

are implemented in OWL (Web Ontology Language: http://www.w3.org/ 2004/OWL). As a derivative of XML, OWL provides standard, open, and extensible data representations as well as a powerful descriptive logic foundation that can be used to represent and reason about semantically rich descriptions of relationships between entities and actions. This provides the ability to reason about relationships between actions and create semantically rich policies. Policies are used to dynamically regulate the behavior of system components without changing code or requiring the cooperation of the components being governed. By changing policies, a system can be continuously adjusted to accommodate variations in externally imposed constraints and environmental conditions.

DISSEMINATION SERVICES

Tactical network environments demand reliable, robust, and efficient approaches to disseminating information that are tolerant to unreliable and bandwidth-constrained networks. DisService [5] is an information dissemination service that is part of the Agile Computing middleware. DisService opportunistically discovers and exploits excess communications, storage, and processing capacity in a distributed network to improve the performance of information dissemination. DisService supports store and forward delivery of data and caches data throughout the network, thereby making it disruption tolerant and improving availability of data. Each node in a network running DisService operates in a distributed, peer-to-peer manner while processing and communicating the published information and requested subscriptions from neighboring nodes. Information is disseminated using an efficient combination of push and pull. These and other capabilities combine to make DisService an effective system for information dissemination in tactical environments.

THE RIGHT INFORMATION

GATHERING THE RIGHT INFORMATION

It has become clear that the role of the Soldier in today's conflict is not simply to find and engage the enemy. While this remains a critical capability, our Soldiers are routinely tasked with a myriad of other tasks such as local security, reconstruction and training local forces to name a few. These types of missions highlight the need to balance the focus on what Major General Flynn [2] refers to as "red" activity – concerning the enemy – with "white" activity – the population, economy, development, and government. It is not difficult to understand that these missions require a greater focus on "white" information, but what is surprising to many is Major General Flynn's conclusion that "white" information is also the key to stopping insurgents. Basically, understanding the needs, motives and fears of the local people can help get at the root of support that enables the insurgence.

The importance of “white” information has several implications. First, the vast majority of white information is unclassified. Second, is that the information will be useful to a larger audience such as Non-Government Organizations (NGOs), Provincial Reconstruction Teams (PRTs), local government and security forces. By enabling support for these types of entities, a force may, in turn be more effective at receiving informational support from them. A third implication is that there is some actionable response embedded in this issue. In other words, we deal with “white” information differently. The way we collect it, the way we use it and the way we share it is fundamentally different. It is interesting to note that this is not limited to what we are referring to as white information. Within current systems, we have a variety of types of information that should also be treated differently. Sometimes this is handled by having separate systems to address each kind of information (e.g. Blue Force Tracker), but most often it is “handled” by simply putting all the information into a single system where it is generally managed uniformly with respect to priority, destination and access. As we try to address the white information, it is clear we will need special handling to enable the unique features of this and other type of special information.

SHARING THE RIGHT INFORMATION

Sharing the right information is about being able to determine relevance. There is an abundance of information flowing through our military, or more accurately stagnating in it. The current reliance on formal reports and completely unstructured text based information and video produces a mass of information but provides no mechanism to make use of the information. Leveraging semantic technology can assist with this.

It is semantics that will be used to derive relevance. Without any semantics our mountain of information is an opaque mass. Semantic labeling of information is something that has been pursued, but is often thought of as impractical, restrictive and burdensome. This is partly because people typically think of post-processing documents or rigid forms that require all fields to be filled correctly. However, much power can be gained by labeling that can be automatically or semi-automatically generated. Both Major General Flynn [2] and General Chairelli [1]state that the Soldier is the best source of information and this means that Soldiers are the entry point for vast amounts of data. They are the ones who will also eventually rely on this information to plan and execute their missions. The fear that adding semantics to data will unduly burden our Soldiers who are already running at maximum capacity is a valid concern. However this does not restrict the possibility of such labeling, it merely adds a design constraint on our future systems. Today’s technology can provide great capabilities to the Soldier in a way that yields enough benefit to outweigh the burden that change unavoidably imposes.

Data entry and data retrieval are inherently coupled and at odds. First the data must be collected and entered into the system in some way. Here the ideal situation is a free form entry tool that requires no effort by the person entering the data. The other side of the problem is retrieving the data from the system for use in analysis and decision-making. Now the ideal situation is that the data is highly labeled, allowing very detailed queries to extract exactly the information needed and nothing else. These two constraints are clearly at odds with each other and suggest that the best solution is most likely a compromise that provides the ability to label data in a meaningful way while minimizing the burden on the information gather that already has a tremendous amount of work to do.

Another important point about sharing the right information is that sometimes the right information is not the data itself, but some small summary or metadata statement about the information. Certain types of data, particularly high bandwidth items with potentially low relevance, need only advertise their availability without burdening the network with their transmission. Then Soldiers can decide for themselves if they are interested and retrieve the information on demand.

THE RIGHT PLACE

GATHERING AT THE RIGHT PLACE

Major General Flynn [2] points out that in today's war, the Soldier on the ground is usually the person best informed about the environment and the enemy, necessitating the need for bottom-up information flow. The emphasis on bottom-up information gathering is a burden to the Soldier, but also provides an opportunity. Since the Soldier is situated in the environment and task, we can leverage this to automatically provide some semantics about the context of any information gathered. Simple examples are geographic position and time. More complex examples involve an understanding of how the current task relates to higher-level missions. Similarly, importance of information can frequently be correlated with the importance of the task. Semantics not only enables automatic dissemination, but also allows for powerful query mechanisms.

Error reduction is another potential benefit. By capturing some data automatically, we can help reduce data entry mistakes. Position and times can be accurately and automatically recorded instead of the Soldier trying to mentally recreate them after the mission. Simple notes (e.g. text, voice, image or video) can be recorded in the field during or close to the occurrence of an event. It is hard to remember everything that happened on a mission, especially under stress. If we can enable the Soldier to capture the information immediately, while it is fresh in his or her

mind that will lead to more accurate information and post mission reports. While we cannot eliminate errors, providing effective tools can help reduce them.

SHARING TO THE RIGHT PLACE

Places can be physical locations, but more frequently we direct information to sets of people, roles, teams, groups, or individuals. While sometimes broadcasting information may be appropriate, it is more often the case that information should be targeted based on the type of information. In today's counterinsurgency environment, we need to be able to share in remote and sometimes austere areas.

We have identified several categories of information that have different needs; mission, information requests, situation awareness, and ASCOPE. While there may be other pertinent groupings, these provide a fairly broad scope and highlight the significant differences in the way Soldiers collect and share information. We will now discuss the needs of each type and how our technologies can be leveraged in support of each.

MISSION

Mission information is that information directly related to the mission planning and execution. It is typically shared up the chain of command and not shared with other entities except occasionally sharing pertinent details with adjacent units to deconflict operations. The normal flow is down and up the chain of command. Currently the mapping and tracking of high level goals to mission tasks is a very manual process. This burdens the Soldier with a complex cognitive task that is frequently exacerbated by ambiguous or redundant messages. Providing even simple semantics to track the relation between high level objectives and mission execution would go a long way to help the process. Although, human interpretation will remain an essential ingredient in this complex task, semantics can be used to help make the process semi-automatic and would provide powerful query mechanisms for future operations. For example, reporting format templates could be used to automatically create reports that include mission details in systems such as TiGR. The Soldier would no longer need to manually input information, potentially in multiple systems, but would simply review the automatic report and add a brief synopsis and commentary as appropriate. Reporting could be autonomously targeted to the correct recipient by specifying this need in the initial task request. In this way, things like schedules, mission results and logistics (e.g. weapon and personnel status) can be routed to the appropriate people instead of being lumped into a large report or having to generate complete reports for each type.

INFORMATION REQUESTS

Information requests, such as Priority Intelligence Requests (PIRs) are a common way to elicit information that may or may not be directly related to the current mission of a particular unit. These differ from mission information because the requestor is not necessarily in the direct chain of command. Unfortunately these requests usually still end up traveling down and up the chain of command. While it is important for the upper levels of command to be aware of all tasks in which their units are involved, this process unnecessarily delays the information sharing process. The responses are typically buried in mission reports instead of being disseminated directly to the requestor. This means that the response can potential be lost and suffers an unnecessary delay en route.

SITUATION AWARENESS

Some information is critical for situation awareness (SA) of the local area. Some examples are improvised explosive device (IED) activity, route obstructions, and resource availability such as an unmanned aerial vehicle (UAV). This type of information differs in that it is relevant outside the normal chain of command, particularly to entities in the immediate geographical area. SA information is also often perishable in that its value diminishes over time, so it is critical to disseminate this information quickly.

ASCOPE

ASCOPE (Area, Security, Communications, Organizations, People and Events) is basically what Major General Flynn [2] has referred to as “white” information. Situation Awareness information may also be ASCOPE, but most ASCOPE is about long term trends and developing an understanding of the big picture of the local area geographically, economically, politically, and socially. The value of this type of information extends beyond the normal chain of command and is pertinent to a variety of entities that Soldiers typically interact with such as NGOs, PRTs, local security and other non-US-military units.

THE RIGHT TIME

GATHERING IN A TIMELY MANNER

Time is one of the most precious and scarce resources to a Soldier. Providing automated and semi-automated tracking, categorizing, and reporting will alleviate some of the administrative burden on the Soldier.

Task tracking is currently a manual process that burdens the Soldier with deciphering duplicate and ambiguous information. Semi-automated task tracking using semantic technology could help reduce this burden. Task could be high-level orders, low-level specific missions or anything in between as well as requests for information. Task tracking could help track the task, who

assigned it, who it was assigned to and the current status. Status updates could be conducted in real-time by leveraging opportunistic resources. They could also help connect the task to higher or lower level tasks to help maintain the correct context and enable better understanding of intent. It could also track reporting requirements. The usefulness of semi-automatic tracking requires proper interface design to ensure these features are simple and accessible to the Soldier. Features like sorting and querying of the tasks will be essential.

Semi-automated reporting can save time and effort. When Soldiers return to base from a mission they are very tired. Even if they remember everything, it takes a lot of discipline to sit down and write a detailed report. As the Soldier collects information in the field, an automated process will simultaneously build both a progressive mission report that is accessible in real-time, and a post mission report that the Soldier can review, edit and publish or archive after the mission. This report can be based on the specified reporting requirements tracked with the task. Much of the mundane data could be automated. For example, a GPS equipped device could record information about the personnel on the patrol, the time of departure, the route, the amount of time spent at each location, etc. Pictures, notes, audio, and video taken in the field can be automatically time stamped, geo-located and associated with the current task. To avoid having Soldiers looking down and spending the time necessary to write legible notes, voice transcription or recording could be a used. Also, the Soldier could record raw audio or video, including dialogue from detainees or local nationals that could be carefully translated and analyzed later. All of this data would be organized and available during the mission and ready for editing as soon as the Soldier sits down to debrief the mission. Getting these technical details out of the way while on the mission allows the Soldier to focus on creating an intelligent, insightful, and accurate post mission analysis as soon as he returns. The pictures and data from the mission can serve to jog the Soldier's memory as he or she writes the report and comments. Semantically connecting reports to requirements also adds task-to-troop accountability. It provides a mechanism to the status of activities with respect to the commander’s intent.

Other types of automatic reporting could include logistics, supply, maintenance, personnel and property accountability. Currently, the Army uses non-automated Power-Point and Excel trackers to keep track of almost all of this. The automated systems that do exist like SAMS-E box and PBUSE are not capable of cross talk, nor are they linked to or available to a wide user group. As a result, Soldiers spend a lot of time updating these countless trackers that are always vulnerable to human error. Furthermore, because none of it is automated, the countless updates mean that different versions or copies of the same tracker often reflect different information and it is impossible to know which one is correct without going back and checking manually. Using personal digital devices, Soldiers would be able to constantly update their own information. Team leaders would update things like the location and status of their Soldiers, accountability of equipment, current levels of supply/ammunition, broken equipment etc. This information would automatically update the master tracker at all levels. When a company commander wants to see how much ammo a platoon has left, he can check it on a personal digital device. The most important point for all of this is *not* that it's a cooler way to perform these logistics functions, but rather that it would free up a tremendous amount of time that Soldiers could use to focus on important things like training, rehearsals, preventative

maintenance and inspections. They currently spend far too much time "counting beans" that could be handled by a computer.

SHARING IN A TIMELY MANNER

Just as radio connectivity provided a decisive advantage on its introduction, digital connectivity has the same potential. The military relies on vast amounts of digital data and networks to support sharing it, so much so it has even coined the phrase “net-centric warfare.” When our Soldiers operate at the tactical edge, they are frequently without this advantage. “The shortage of bandwidth is one of the greatest challenges in Afghanistan today. Along with the growth in communications requirements, advances in collaboration, information sharing, and peer-to-peer style communications …are also changing the way traffic flows at the tactical edge [5].”

Currently, digital data is shared by entering it into one of the Army’s many systems. This usually means that in order to have the best pre-mission information, Soldiers have to check each of those systems before they depart for a mission, and then enter their own data when they return. During the mission, with very limited exceptions (i.e. FBCB2), they are disconnected digitally even if they are within sight of another unit. Though providing worldwide reliable network connectivity to each and every soldier is currently impractical, we can support digital sharing among team members and even among geographically close neighboring units. This can be done through MANETs (Mobile Ad-Hoc Network) that will need to form automatically, in an ad hoc manner to allow peer-to-peer communication. The MANETs will clearly be transient and the infrastructure must support that. As units move into and out of range of one another, the Soldiers need an infrastructure to manage the connections and handle the data sharing without needing the Soldier’s attention. Our dissemination service meets this need. It provides peer-to-peer sharing of information as it is being gathered by Soldiers in the field. In this open ad hoc environment, controlling data flow and access will be critical. Policy restrictions and prioritization concerning what is shared with whom are critical to making this kind of opportunistic sharing work. General policies can be set up ahead of time to guide the sharing process. These policies could be modified dynamically to support the changing needs of a situation. This type of lateral information exchange can provide a great speed advantage over the current approach. It also enables the potential for harvesting of data opportunistically by available resources (e.g. passing units, UAV, etc.).

Sharing in a timely manner also means supporting timely requests. We see a great value in providing the Soldier with a mechanism for dynamically generating requests and automatic cueing. To allow each unit to have the ability to dynamically request specific information, potentially directly would be useful. Additionally, cueing the Soldier when desired information has become available would be very useful.

Lastly, reporting is a very large demand on the Soldiers. Up the information chain, users want data tied to objectives, missions and requests. Semantics can make this connection explicit. Instead of an offline rigid reporting form, we could provide an automatically populated form

with the potential to elaborate as necessary. We see this type of system helping the Soldier to deal with the various information systems currently deployed. It could translate the data gathered into the appropriate format for interfacing with TIGR, CPOF or any other system.

EXAMPLES OF HOW THESE TECHNOLOGIES CAN HELP MEET "RIGHT INFORMATION – RIGHT PLACE – RIGHT TIME"

PLANNED EXCHANGES OUTSIDE THE WIRE

Occasionally units may plan to coordinate outside the wire. Currently this would mean coordination over the radio or potentially exchanging written notes. Given today's digital capabilities and the bottom-up nature of information flow, it makes sense to provide a mechanism for data sharing outside the wire. Units should be able to automatically detect when they are in range with one another and exchange pertinent information digitally. We provide this mechanism through our Dissemination Service.

OPPORTUNISTIC EXCHANGES OUTSIDE THE WIRE

Similarly, a unit may encounter another unit that it had not planned to coordinate with. While the mission information may not be relevant, situation awareness information would definitely be. For example, a local unit could provide a passing convoy information on the current status of roads and bridges in the local area and potentially their assessment of IED activity along different routes. Again, we would provide the connection mechanism through our Dissemination Service and manage what gets sent between units (i.e. SA information in this case) through KAoS Policy Services.

HARVESTING

Information harvesting can also be enabled through the same envisioned technology. While a Soldier may not want mission information harvested until the mission is complete, any PIR and SA would be very appropriate for harvesting to allow potentially faster distribution. The harvester could connect using the Dissemination Service and KAoS Policy Services would control what actually gets passed.

PERMANENTLY DISJOINT ENTITIES

Some entities will never be connected to military information system such as CPOF. Local security forces, NGOs, and other non-military organizations are currently not included. It would be beneficial in building relations with these types of entities to be able to share appropriate information. It is very likely that these elements will at some point advance to using some type

of digital information system. If provided with the Dissemination Service, we could use KAoS Policies to control the type of information shared. When units meet with or visit these organizations, they could potentially share and collect information.

TARGETED DELIVERY

One nice feature of our services is the ability to provide targeted delivery. Information is sent only to the person of interest. Many current systems only allow for broadcast, relying on the recipient to actively seek the response. Our services allow for broadcast, but also support targeted delivery.

REAL-TIME AD HOC COORDINATION

An added bonus of leveraging services like our Dissemination and Policy Service is that it enables real-time ad hoc coordination between units. Our services can be configured ahead of time to limit the burden on the Soldier and handle the typical workflow, but they can be dynamically adjusted to meet the changing needs of the Soldier. Smaller ad hoc work groups can be formed to rapidly and privately share information for immediate collaboration. (Can we demonstrate this? What would it take?)

WHERE DOES ALL OF THIS FIT

Currently information is shared over several systems such as Tactical Ground Reporting (TIGR), Distributed Common Ground System – Army (DCGS-A), Combined Information Data Network Exchange (CIDNE), Command Post of the Future (CPOF), FBCB2 and Blue Force Tracker and Joint Battlefield Viewer (JBV), and a variety of digital air-space management tools. Each of these systems fills a niche but none cover the full spectrum of conflict/action that our military operates within. FBCB2/BFT is excellent for high intensity conflict; CIDNE is great to track SIGACTs, CPOF gives a fair comprehensive picture of the COE, etc. Additionally, many of these systems live “inside the wire,” meaning the Soldier only has access to the system while on some base facility with a wired connection to the secret military network, SIPRNET. FBCB2 and Blue Force Tracking are exceptions, but are typically limited to position and text message data only. Lastly, these systems are all classified information sources, which means access to information by foreign military and police forces, non-governmental organizations and other non-US military sources is not possible.

What we are proposing is a set of technologies to support the individual Soldier digitally “outside the wire.” The semantic technologies help the Soldier track and organize their activities. The policy-managed information sharing in dynamic peer-to-peer environments provides the decisive advantage of digital connectivity. This opens many new opportunities as

discussed in the previous section. Lastly, though we do not currently support it, this type of tool could be the interface to the myriad of information systems the Soldier must deal with.

POTENTIAL PROBLEMS

Some potential problems we see are that gathering data while on patrol can be hazardous. You don't want to put down your gun to take a picture. However, most soldiers spend more time taking pictures and writing notes then firing bullets and maneuvering on an enemy. Gathering occurs anyway, just not in a way that permits automatic semantic mark up or immediate sharing. Another way to look is to consider whether a Soldier would ever want to pass some information along while "outside the wire" and would it have been nice if that Soldier had a tool to enable that automatically instead of having to stop what he or she was doing and focus on setting up communications to pass the information. Another challenge to supporting the soldier digitally "outside the wire" is the potential for enemy interruption of services. Then we are back to where we are now, relying on hand notes and memory. The last problem we will mention is system compromise. What happens if the system falls into the hands of an enemy or another foreign entity. This is a hardware security issue that falls outside the scope of this work, although policy services could be used to block the compromised device from further access.

DEMONSTRATION

Our demonstration will try to show the potential of leveraging semantic technologies and our KAoS policy managed DisService. We will show how we envision semantic technologies helping the Soldier track and organize their activities. We will also demonstrate various opportunities provided by the policy-managed information sharing in dynamic peer-to-peer environments. Our demonstration will be a prototype of the envision hand held digital system, similar to an iPhone, and will demonstrate several of the key features. We will demonstrate how simple semantics can be provided through a hand held device with minimal burden to the Soldier. We will show how KAoS policies can be used to control data access and prioritization. We will also show managing information flow in dynamic ad hoc networks using DisService.

The demonstration will be in the context of a hypothetical scenario typical for our Soldiers. We will use a hypothetical operations order and corresponding task list to generate semantic relations between the different levels of tasking. After organizing potentially several tasks and missions, the Soldier selects the current task and initiates it with the press of a button. Time and position are automatically recorded throughout the mission. Events can be marked at the press of a button and then expanded on immediately or at a later time. The data collected (e.g. pictures, video, voice notes, etc.) is automatically associated with the selected task. The Soldier can modify this association if events occur that are different from the context of the current task (e.g. SA, PIR or ASCOPE). We will show two overlapping patrols exchanging information

outside the wire. We will show PIR information being harvested and returned to base ahead of the patrols return. We will show one of the patrols meeting with a local tribal leader and exchanging ASCOPE information. We will show the patrol opportunistically sharing information with a passing convoy about local route safety. We will also show real-time coordination between two adjacent units. Upon return to base, a rough draft of the mission report is automatically generated. The Soldier simply reviews and modifies the report as necessary before sending. Other types of data may not need any action by the Soldier at all. If a Soldier sees something that is a priority intelligence request, noting it as such can cause it to automatically be routed to the authority that made the request without any other action by the Soldier. Similarly, ASCOPE information can be routed to anyone interested in that type of information, potentially even NGOs. We will show how this all can occur "outside the wire" in a peer-to-peer manner with policies managing the flow of information.

CONCLUSION

To enable timely and effective information sharing in today's counterinsurgency environment we highlight three technology capabilities. Semantics help relate information and enable automation. Our KAoS policy service can be used to manage access to data and provide data sharing prioritization. And finally, our Dissemination service allows for ad hoc communication networks to be formed and disbanded seamlessly outside of normal wide area network support.

We have discussed how these technologies can meet the goal of "Right Information – Right Place – Right Time." In order for a machine to understand which information is the "right information" some labels or semantics are needed. In this way, semantics make information actionable. These semantics can then be leveraged by our services to get information to the "right place." The place can be a set of people, roles, teams, groups, or physical locations. KAoS policy services ensure it is delivered only to those it is designated for and the Dissemination service enables that distribution to occur "outside the wire" in a peer-to-peer manner. The semantics can also help ensure the "right time" by enabling KAoS policy services to prioritize the information. The Dissemination service also helps meet the "right time" by allowing peer-to-peer sharing and opportunistic harvesting potential.

In the end, we must provide tools that support the Soldiers digitally as they travel "outside the wire" into deployed tactical environments that can be austere and remote. This is particularly important given the double burden a Soldier bears in a counterinsurgency as both the producer and consumer and the information gathering requirements in today's counterinsurgency environment.

REFERENCES

[1] General Peter Chiarelli, Vice Chief of Staff, Army; "U.S. Army Modernization Program" brief for AUSA/ILW breakfast, 10 September 2009.

[2] Major General Michael T. Flynn (USA), Captain Matt Pottinger (USMC), Paul D. Batchelor (DIA); "Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan", in Voices From the Field, January 2010

[3] L. Bunch, J.M. Bradshaw, C. Young; "Policy-Governed Information Exchange in a U.S. Army Operational Scenario"

[4] A. Uszok, J.M. Bradshaw, M. Johnson, R. Jeffers, A. Tate, J. Dalton, and S. Aitken. "KAoS policy management for semantic web services." IEEE Intelligent Systems 19, no. 4 (July/August 2004): 32-41.

[5] N. Suri, G. Benincasa, S. Formaggi, R. Winkler, S. Choy, J. Kovach, L. Tokarcik; "DisService:A Peer-to-Peer Information Dissemination Service for tactical Environments", August 2008

[6] R. Osborne, J. Barrows; "At the Tactical Edge", Military Information Technology, volume 13, issue 2, 2009