12th International Conference on Information Fusion
Seattle, WA, USA, July 6-9, 2009

An End to End Life Cycle for ISR in Coalition Networks*

Dinesh Verma
IBM T.J. Watson Research Center
Hawthorne NY, U.S.A.
dverma@us.ibm.com

Tien Pham
Gregory H. Cirincione
U.S. Army Research Laboratory
Adelphi MD, U.S.A.
tien.pham1@us.army.mil
greg.cirincione@us.army.mil

Gavin Pearson
Defence Science & Technology Laboratory
Porton Down, Dstl Porton Down,
Salisbury, Wiltshire SP4 0JQ, U.K.
agpearson@dstl.gov.uk

Abstract – Coalition Intelligence, Surveillance and Reconnaissance (ISR) networks provide an invaluable service to joint missions and operations provided they are installed and operated appropriately. The process of obtaining the benefits of an ISR network needs to begin long before the first shared ISR asset is deployed on the ground. The joint mission needs to be planned so as to satisfy any policy constraints and national objectives individual participants may have, and the right mechanisms for sharing information need to be developed. Policy conflicts that may prevent optimal operation of the network need to be resolved at the appropriate level of authority. In this paper, we present an end-to-end life-cycle for planning and deploying a coalition ISR network. This life-cycle model is targeted to address the requirements that arise due to the differences policies and national objectives of different partners in a coalition.

Keywords: policy-based security management, network planning, mission planning, sensor network operation, ISR, coalition operations.

1. Introduction and Motivation

The assembly and dynamic control of ISR sensors, platforms and networks to support multiple concurrent coalition missions is a complex operation due to differences in technology, methodologies and policies that exist among different partners of the coalition. Coalition operations usually entail an *ad hoc* arrangement between two or more organizations acting together in pursuit of a common objective. Each organization within a coalition has its own inherent restrictions on how it is allowed to operate. These restrictions are usually stated as a set of policies. Within such an *ad hoc* coalition, *ad hoc* Communities of Interest (CoI's) come together, perhaps for only a short time, with different sensors, sensor platforms, data fusion elements, and networks, to conduct a task (or set of tasks) with different coalition members taking different roles.

Coalition forces conducting distributed ground operations in complex and urban terrain need reliable and actionable information from a "network" of Intelligence, Surveillance and Reconnaissance (ISR) assets. Currently, this remains to be a major challenge for coalition forces conducting operations in theaters when considering disparate ISR assets (e.g., sensors, sensing platforms, signal intelligence/human intelligence, data fusion elements, secure networking, etc.) and associated policies (e.g. security, resource control, command & control (C2), etc.). In addition, the different levels of trust between US, UK and other coalition partners add to the complexity of interoperability and the overall challenge.

Current research in sensor networks tends to focus on the physical aspects of networking such as bandwidth, power and scalability, while current research in security & policy tends to focus on automated policy-based security and/or efficient mechanisms (e.g., authentication, integrity, access control, non-repudiation, etc.). By jointly developing technology to address both aspects for networks of ISR assets and working with the users (e.g., troops, analysts and mission planners), the sharing/dissemination of critical and timely information to coalition ground forces can be realized.

In order to execute such short-term coalition ISR operations efficiently, the operation needs to be planned, deployed and operated while being cognizant of the differences that may exist among different organizations. Towards that goal, developing a structured life-cycle model of such operations, and delineating the steps that ought to be taken at each step of the life-cycle can increase

* This research was sponsored by the US Army Research Laboratory and the UK Ministry of Defence and was accomplished under Agreement Number W911NF-06-3-0001. The views and conclusions contained in this document are those of the author(s) and should not be interpreted as representing the official policies, either expressed or implied, of the US Army Research Laboratory, the US Government, the UK Ministry of Defence or the UK Government. The US and UK Governments are authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation hereon. This paper includes British Crown copyright material.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUL 2009		**06-07-2009 to 09-07-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
An End to End Life Cycle for ISR in Coalition Networks	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **IBM T.J. Watson Research center, , ,Hawthorne,NY**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM002299. Presented at the International Conference on Information Fusion (12th) (Fusion 2009). Held in Seattle, Washington, on 6-9 July 2009. U.S. Government or Federal Rights License.

14. ABSTRACT
Coalition Intelligence, Surveillance and Reconnaissance (ISR) networks provide an invaluable service to joint missions and operations provided they are installed and operated appropriately. The process of obtaining the benefits of an ISR network needs to begin long before the first shared ISR asset is deployed on the ground. The joint mission needs to be planned so as to satisfy any policy constraints and national objectives individual participants may have, and the right mechanisms for sharing information need to be developed. Policy conflicts that may prevent optimal operation of the network need to be resolved at the appropriate level of authority. In this paper, we present an end-to-end life-cycle for planning and deploying a coalition ISR network. This life-cycle model is targeted to address the requirements that arise due to the differences policies and national objectives of different partners in a coalition.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Public Release**	**7**	

the effectiveness of coalition operations. The objective of this paper is to describe such a life-cycle which can be used effectively for successful execution of coalition ISR operations.

Section 2 of this paper describes the structure and organization of a coalition ISR network that we assume for the purpose of this paper. Section 3 provides an overview of the life-cycle and discusses each of the stages of the life-cycle. Section 4 describes a scenario for coalition operations. The next several sections present the technical needs of the coalition CoIs in each of the life-cycle stages. Finally, we draw our conclusions.

2. Enhanced Information Fusion

An ISR network is an adaptive ad-hoc network of ISR sensors, other sources of data (e.g., humans), platforms, communication systems, etc., that provides actionable Information and Intelligence (I2) to its customers. The sensors may exhibit heterogeneity in a variety of dimensions including passive or active, field of view and regard, range and modality (e.g., biometric, acoustic, radar); similarly, there may be significant heterogeneity in the other elements of an ISR network.

ISR sensors for distributed ground operations can be categorized into low-resolution or "activity" sensors and high-resolution sensors. Activity sensors are typically inexpensive, passive and low-power sensors. They usually provide persistent sensing and broad-area coverage. Some of the commonly used activity sensors are acoustic, seismic, magnetic, passive infrared, and chemical/biological. To enhance the probability of detection while reducing the probability of false alarm, multi-modal fusion is used in many sensor systems to obtain orthogonal and complementary information. For example, multi-modal fusion of several activity sensors is used to detect and classify personnel and human activity [1]-[2]. High-resolution sensors are generally more expensive, active and/or high-power sensors. Examples would be day-night video and electro-optic cameras and imagers.

For distributed ground operations, Unattended Ground Sensors (UGS) [3] have become reliable and frequently used ISR systems. UGS systems can be employed/deployed to cover large areas in open terrain (e.g., border region) or in restricted areas such as urban environments, and used in several scenarios [4].

As the coalition operations become more dynamic in complex environments, multi-modal sensor systems need to be distributed in space and in time. As such, the mobile ground and aerial sensing platforms are becoming more important. For ISR applications, the mobile ground platforms include military Humvees, unmanned ground vehicles (UGV's) and small robotic vehicles (e.g., Packbot) [5]; and aerial platforms include unmanned aerial vehicles (UAV's) and aerostats [6]. These mobile platforms often provide area coverage gaps or ad-hoc network connectivity; carry expensive high-end/high-resolution sensor payloads; are shared assets supporting multiple missions; are tasks to move to the locations of interest for further ISR information gathering or confirmation; and/or provide communication relays or links for exfiltration of ISR information.

2.1 Coalition ISR Networks

In a typical coalition operation, an ISR community of interest (CoI) is dynamically formed to conduct joint coalition operations [7]. The ISR CoI will operate across a number of levels of command, and will thus include a number of more focused CoI's within the overall CoI. One way to define and manage access control within dynamic coalition CoIs is with the use of role based access control [8].

An ISR CoI can be an ad-hoc team consisting of several coalition partners executing many concurrent missions. Such missions include border/perimeter reconnaissance and surveillance, camp site surveillance, and detection/classification of human activities in concealed/confined spaces or locations of human infrastructures. A CoI brings together a set of ISR assets, specific missions, and sets of policies that govern information security and fusion and sharing/dissemination of information.

In any coalition operation actually undertaken, the CoI will include war-fighters and support personnel of various levels. In the context of this paper, we are restricting ourselves to a CoI that is responsible for planning and operation of ISR networks. This CoI will have a supporting role for the other CoIs that are engaged in the operations.

When the CoI needs to establish its own ISR network to conduct its operations, it can draw upon the set of assets that are available on one or more partners in the coalition. A partner may be willing to share some of the ISR assets with other partners in the CoI, while it may want to keep either some assets or information from some ISR assets restricted to its own use, or for use only within a subset of coalition partners. The coalition ISR network needs to be designed to satisfy the guidelines and choices of individual coalition partners.

In current practice, much of the coalition networks are operated and planned in an ad-hoc manner. However, if one postulates a life-cycle model and tries to follow the life-cycle stages in the design and operation of the network, the network can be operated in a better manner and satisfy all requirements and constrained imposed by individual nations making up a coalition. In the next

section, we propose a life-cycle model towards this goal. The life-cycle described draws upon the concept of hierarchical CoIs to model the needs and requirements of a coalition ISR Network.

3. The Coalition ISR Network Life Cycle

A life-cycle describes the stages through which a system moves, and examining the different stages in the life-cycle of a system can provide valuable insights into how the system ought to be developed. Life cycle models have been used in many different fields of computer science, e.g. in planning the development of software systems, and in project management. However, the concept of the life-cycle has not been applied in the context of coalition ISR networks. In this paper, we present a life-cycle model that can be used to satisfy all the requirements of a coalition ISR network. Such a model is shown in Figure 1. As shown in the figure, the life-cycle of the coalition ISR network consists of four distinct stages. At different stages of the life-cycle, the CoI that is involved in ISR coalition network design may be different.

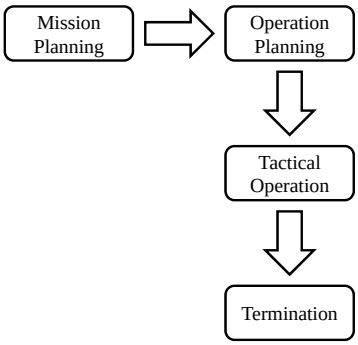

Figure 1. Life Cycle of Coalition ISR Network

In the *mission planning stage*, a CoI from the forces from different coalition partners come together to negotiate and develop the common operating principles and policies that would apply to coalition information flows and any ISR assets that may be shared during coalition operations. At this stage, the ISR networks and systems are not necessarily fully deployed, established or operational in the area of operation. However, each partner in a coalition would have an inventory of ISR assets that they are willing to share/deploy for coalition operations and allow limited visibility to other coalition partners to that inventory and its capabilities. We can refer to the CoI in this stage as the CoI of coalition mission planners.

In the *operation planning stage*, the coalition forms another CoI, which is distinct from the CoI of coalition mission planners. The CoI now consists of the members from different coalitions which come together to design and plan the structure of the coalition ISR network that will be deployed in the area of operation. This CoI of operational planners has a relationship to the CoI of mission planners in the sense that the CoI of operational planners needs to follow the policies that have been established by the CoI of mission planners.

The operation planning CoI would be tasked to plan how to undertake and execute the mission. During this stage, the CoI would need to determine the nature of the ISR network they need. They would need to find out the optimal set of ISR assets and the network configuration of those assets that they may need in order to perform the tactical operation.

Yet another CoI, the operator CoI, would be formed in the *tactical operations stage*. In this stage, the ISR networks are deployed and available for operation. The different ISR networks would be interconnected through policy-enabled gateways. These gateways would enforce any policy constraints that are applicable as information flows between different ISR networks. The CoI consists of the administrators and operators that would need to operate and run the installed ISR network.

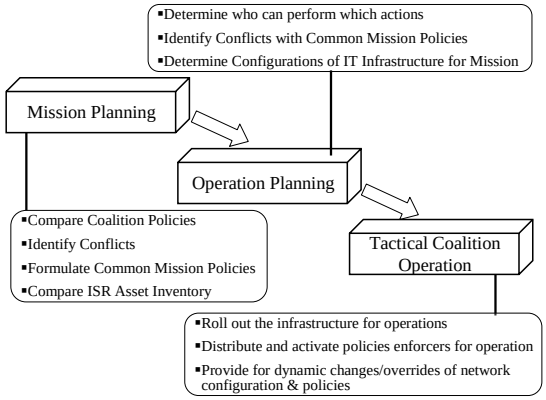

Figure 2. Operations in different Life Cycle Stages

Each operation needs to end, and the coalition ISR network may need to be terminated at the end of the operation (*termination stage*). In this case, the operator CoI needs to retrieve the assets from the area of operation, and return the assets to respective coalition partners. Any data retention and end-of-life policies related to disposing of data and information would need to be complied with.

4. Example Scenario

Let us consider a peace support operation in which US and UK coalition forces have been deployed into a mythical country Holistan to assist the indigenous Government forces in deterring an active insurgency and reassuring the local population. The scenario of Holistan

is described in [9]. In such a case the Coalition (of UK, US and possibly Holistan) forces must operate together to (a) protect the forces in the region and (b) dominate the region (to protect and support local population, and deter/defeat the insurgency).

When operating in the area where the insurgents are known to be active, the US and UK have established their independent base camps. Each of these camps would have their own ISR networks and other infrastructure accessible only to members of the respective coalition partner. However, in order to track insurgents in areas that lie outside the base camp of either army, the coalition members realize that they would need to establish an ISR network which would be owned and operated by the coalition members jointly.

Following the life-cycle model described in Section 3, the following steps will be taken during each of the four stages of the life-cycle.

During the mission planning stage, the military planners from both base-camps meet together. The planners form the CoI at this stage. The CoI anticipates a number of coalition operations to be undertaken, and a number of coalition ISR networks to be installed. The members of the CoI negotiate a set of policies to be applied to coalition operations and share their inventory of ISR assets (with any applicable restrictions) to each other.

Subsequent to this, different coalition operations would need to be undertaken. We restrict ourselves to coalition operations that require the formation of an ISR network from coalition assets. Each such operation passes through an operational planning stage and a tactical coalition operation stage.

During the operational planning stage, the CoI of operational planners have agreed to establish a coalition operation to monitor some area jointly. The members of the CoI work together to determine the best ISR assets to use for the coalition operation, the best way to deploy the assets into a network, and to determine the roles and responsibilities of different members staffing the coalition ISR network

During the tactical operations stage, the coalition ISR network is deployed and the three ISR networks (US, UK and coalition) are interlinked together. Information flows across the networks subject to agreed upon policy constraints, roles and responsibilities. The CoI in this case consists of the operators and users of the coalition ISR network.

During the termination stage, when the ISR network is being dismantled, the CoI of operators would retrieve the assets belonging to the respective organizations, perform any required audits for the inventory and data and return them to the assets of the respective base-camps.

At each stage in the life-cycle, the CoI has different technical needs and requirements. The software assets and tools that satisfy the requirements of the CoI require different properties. In the next several sections, we outline the technical requirements of the software assets that can assist the CoIs in different stages of the life-cycle.

5. Mission Planning Stage

In the mission planning stage, the US, UK and Holistan military planners need to negotiate the policies that will govern the coalition ISR networks. Each country has its own national policies, and the coalition networks need to operate according to the policies. When policies are in contradiction, the planners need to agree how to resolve the contradiction in these policies.

As described in [10], for each member of the coalition operation, the national policies may include the following types of policy sets:

(i) *ISR Asset Characteristics Exchange*: These policies dictate which assets from the asset of a nation may be disclosed to the other partners, and to what extent. A nation may not want to expose existence of sensitive assets to other partners.

(ii) *Local Command and Control (C2) policies*: These are policies that delineate the command structure, their roles, their authorizations, and their obligations including who can develop and modify missions, taskings, and operational policies.

(iii) *Platform Control Policies:* Policies that define whom, with what authentication, and under what conditions platforms (e.g. UAV's, UGV's, robotic vehicles, etc) can be controlled, configured, moved, and re-tasked.

(iv) *Sensor and Sensor System Control Policies*: Policies that define whom, with what authentication, and under what conditions sensors and sensor system can be controlled, configured, moved, re-tasked.

(v) *Sensor Information Access Control Policies*: Policies that define whom (person, C2 element, data fusion element, etc), with what authentication, under what conditions, and in what form (i.e., raw, processed, fused) sensor information can be accessed.

(vi) *Information Flow Protection Policies*: Policies that define how information flows are to be secured and protected confidentiality, integrity, etc.) on any operational network.

(vii) *Information Dissemination Policies:* Policies that describe the conditions/events under which information must be sent and to whom; the conditions and to whom information can be provided when queried

In addition to these, some coalition partners like Holistan may have sensor placement policies. These policies may dictate that certain type of assets may not be placed on some areas. As an example, Holistan may not want a sensor placed in close proximity to a place of religious worship which may be viewed as sacrilege by the population and provide material to fuel the insurgency.

Planners from each nation would need to keep a subset of their policies private to themselves and not share it with other members in the coalition. As an example, it is highly likely that ISR Asset characteristics Exchange policies will not be shared with partners. Depending on the specific nature of the policies, the other types of policies may be shared or not shared.

The mission planners from all countries would need a capability that would allow them to negotiate policies with each other while keeping their national policies (or a subset thereof) secret. Thus, one can envision a scenario where the planners from each country has their own consoles, which allows them to see their national policies, and offer a policy set as tentative policies to other coalition partners. The software on the console must be able to receive policies from other planners, and check for any conflicts among the offered policies and their own national policies. The transfer of a offered policy sets among the different planners may be enabled by means of file transfers among the CoI members, or by the establishment of a simple gateway that allows communication among the CoI members.

Furthermore, the mission planners would need to have an inventory tool which they can use to determine the set of assets that will be offered for coalition ISR networks. Each planner should have visibility to only the assets and capabilities that can be shared subject to their national policies. They should be able to view the inventory offered by other partner. After the set of policies are determined, a set of inventory assets available from all of the coalition members should be visible to each coalition partner.

Some coalition partners, e.g. Holistan, may not have their own inventory software or sensor policy management software. Any software used by mission planners must be able to support policies and inventories (if any) from such coalition partners.

6. Operations Planning Stage

In the operations planning stage, the CoI consists of members who have gotten together to plan and design an ISR network. This CoI will be operating under the control of the set of policies that were negotiated and agreed upon during the mission planning stage.

For example, the US Operations Planner and the UK Operations Planner meet to determine the optimal configuration for a coalition ISR network set up at the coalition campsite and the necessary interconnection between the ISR networks of the two countries. They have a common view of coalition assets and an inventory of assets that the coalition members are allowed to use.

At this stage, the operation planners need to make several decisions. One of these decisions is for the planners to create policies by which the planned coalition ISR network will interoperate with the US and UK networks. These set of policies need to be compatible with the policies which were negotiated previously. Thus, the operations planner would need a policy authoring tool that will allow them to define the effective policies for the planned coalition network, and checks compliance with the coalition policies that have been provided to the software tools [11].

The next decision for the planners is to choose the set of ISR assets from the coalition inventory that ought to be used for the design of the coalition network. In order to meet the specific challenges of ISR (or ISTAR) [12], the planners would need an asset matching tool implementing algorithms for sensor selection schemes [13]-[17]. The asset matching tool selects the right subset of assets from the coalition inventory, depending on the requirements of the mission that is planned.

A third decision to be made at each stage is the actual layout and design for the ISR asset network. For this goal, the planners would need a network planning tool [18] to determine the optimal deployment for the selected ISR assets in the network. This tool should enable them to visualize the ISR coalition network, suggest optimal placement of each asset in the ISR network, and also provide for the location of gateways which would connect the ISR network to the base camp networks of US and UK.

The operations planner would have access to the inventory of coalition ISR assets. However, since there may be multiple coalition networks that may need to be setup, the inventory needs to be updated to show which assets are actually available and which may have been used by another active mission. Towards this goal, an inventory management system needs to be setup for planning the difference coalition networks. Assets are marked as being in use in the inventory tool when they are used for a new network being planned, and marked available when the ISR network is terminated.

After the network is planned and the inventory system updated, the operational policies need to be translated into the configuration of the different assets that make up the coalition ISR network. A policy management tool that

would translate the operational policies for information flow, information dissemination and sensor/platform control needs to be used to convert the policies into the configuration of different devices.

The output from the operations planning stage would be a design for the ISR coalition network, along with the details of the locations where the ISR assets need to be placed, and the configuration of each of the components of the ISR network.

7. Tactical Coalition Operations Stage

During the coalition operation stage, the coalition ISR network is operational. The different assets have been placed on the area of operation (this process is manual in most of current operating conditions) and are interconnected by a sensor network. In order to operate effectively at this stage, the coalition needs an agile sensor network that can handle the different conditions in the area of operation.

In the operational stage, the network may change dynamically as elements of the sensor network may fail, may not be connected, or destroyed. Furthermore, there will be a paucity of skilled network administrators during the actual operations. Thus, the network elements must exhibit self-configuration behavior.

During the deployment of the sensor network, the operator of the network would take the policies/configurations developed during the operations planning stage and load them into the configuration of the corresponding ISR asset or network element. These preconfigured elements are then placed on the different locations recommended by the operational planners. Once these network elements are turned on, they should be able to identify other network elements, associate with them and enable information flows between the ISR coalition network and the existing networks in the base camps of the two countries for example in accordance with the agreed upon set of policies [19].

If the network changes during the operation, the system would need to automatically reconfigure and allow the flow of policies to the users to the maximum extent possible. This requires the development of an agile sensor network (e.g. [20]) that enables the flow of messages at a logical layer even as the underlying physical network changes.

8. Termination Stage

In the termination stage, the ISR network is decommissioned. Different nations may have their own policies for how the decommissioned assets need to be handled. However, at a minimum, the information in the coalition asset inventory tool needs to be updated so as the set of available assets for new ISR networks to be planned are correct.

In addition to updating the inventory, the termination stage may require an after action review of the policies that were used in the operational stage, specially a review of the occasions where policies needed to be modified in the field. An assessment of the operational stage may result in an reassessment and reevaluation of the coalition policies that were agreed upon in the mission planning stage.

9. Conclusion

In this paper, we have introduced a life-cycle model for the planning and operation of coalition networks. The life-cycle model describes the different stages that a coalition ISR network ought to go through, and describes the technical needs of the coalition CoI which is formed and supported at each stage of the life-cycle. The life-cycle model allows us to determine and develop a set of software tools to support coalition operations, and enables us to research and develop algorithms that enable better functioning of those software tools.

10. References

[1] T. Damarla, L. Kaplan, and A. Chan, "Human infrastructure and human activity detection," in *Proc. of ISIF Fusion 2007*, Quebec City, Quebec, Canada

[2] R. Damarla and D. Ufford, "Personnel detection using ground sensors", *Proc. of SPIE Unattended Ground, Sea, and Air Sensor Technologies and Applications IX*, - Vol. 6562 , May 2008.

[3] M. Kolodny, "The Family of UGS," *Military Sensing Symposium on Battlefield Acoustics & Magnetic Sensors Symposium*, Laurel, MD, Aug 2007.

[4] N. Srour and T. Pham, "Acoustic UGS for Today's Battlefield," *NATO SET-107 Symposium on Battlefield Acoustic Sensing for ISR Applications*, Amsterdam, the Netherlands, October 2006.

[5] S. Young and M. Scanlon, "Acoustic sensors on small robots for the urban environment," *Proc. of SPIE Vol. 5804 -- Unmanned Ground Vehicle Technology VII*, May 2005.

[6] T. Pham, "Acoustic Sensing for Urban Battlefield Applications," *Proc. of 19th International Congress on Acoustics*, Madrid, Spain, Sept 2007.

[7] E. Asmare, S. Calo, et al, "Secure Dynamic Community Establishment in Coalitions," *2007 MILCOM*, Orlando FL, Oct 2007.

[8] A. Schaeffer-Filho, J. Lobo, et al, "A Role-based Infrastructure for the Management of Dynamic Communities," *9th IEEE International Workshops on Policies for Distributed Systems and Networks*, Palisades NY, June 2008.

[9] D. Roberts, G. Lock, & D. Verma, "Holistan – A Futuristic Coalition Scenario for International Coalition Operations," *Proc. Fifth International Conference on Knowledge Systems for Coalition Operations*, KSCO-2007, Waltham, MA, May 2007.

[10] T. Pham, G. Cirincione, D. Verma and G. Pearson, "Intelligence, Surveillance, and Reconnaissance fusion for coalition operations," *Proc. 11th International Conference on Information Fusion*, FUSION 2008, Cologne, Germany, July 2008.

[11] C. Brodie et. al., "The Coalition Policy Management Portal for Policy Authoring, Verification and Deployment,", *IEEE Workshop on Policies for Distributed Systems and Networks*, POLICY 2008, June 2008, Palisades, NY.

[12] G. Pearson, "A vision of network-centric ISTAR and the resulting challenges," *SPIE Defense & Security Symposium: 6562 Unattended Ground, Sea, and Air Sensor Technologies and Applications X*, Orlando, FL, March 2008.

[13] H. Rowaihy, et al, "A Survey of Sensor Selection Schemes in Wireless Sensor Networks," *Proc. of SPIE Vol. 6562 Unattended Ground, Sea, and Air Sensor Technologies and Applications IX*, May 2007.

[14] A. Preece, et al, "Matching sensors to missions using a knowledge-based approach," *SPIE Defense & Security Symposium: Defense Transformation and Net-Centric Systems Conference*, Orlando, FL, March 2008.

[15] M. Gomez,et al, "An Ontology-Centric Approach to Sensor-Mission Assignment," *5th European Semantic Web Conference*, Tenerife, Spain, June 2008.

[16] H. Rowaihy, M. Johnson, A. Bar-Noy, T. Brown and T. La Porta, "Assigning Sensors to Competing Missions," *Proc. IEEE Globecom* 2008, New Orleans, LA, USA, December 2008.

[17] A. Preece, et. al., *Reasoning and Resource Allocation for Sensor-Mission Assignment in a Coalition Context*, in MILCOM 2008, San Diego, CA, USA, November 2008.

[18] K. Romer and F. Mattern, "The Design Space of Wireless Sensor Networks," *IEEE Wireless Communications*, Dec. 2004, vol 11, no. 6, pp. 54-61.

[19] D. Verma, et al, "Policy enabled interconnection of sensor networks," *SPIE Defense & Security Symposium: Defense Transformation and Net-Centric Systems Conference*, Orlando, FL, March 2008.

[20] F. Bergamaschi et. al. "Policy Enabled ITA Sensor Fabric: A Distributed Framework for the Validation of Experimental Algorithms Using Real and Simulated Sensors," *IEEE International Workshop on Policies For Distributed Systems and Networks*, June 2008). Palisades, NY.