Information Sharing and Security in Dynamic Coalitions

Charles E. Phillips, Jr.
Computer Science & Engineering Dept.
191 Auditorium Road, Box U-155
The University of Connecticut
Storrs, CT 06269-3155
Tel: 860.486.5582 Fax: 4817
charlesp@engr.uconn.edu

T.C. Ting and Steven A. Demurjian
Computer Science & Engineering Dept.
191 Auditorium Road, Box U-155
The University of Connecticut
Storrs, CT 06269-3155
Tel: 860.486.4818 Fax: 4817
{steve, ting}@ engr.uconn.edu

ABSTRACT
Today, information sharing is critical to almost every institution. There is no more critical need for information sharing than during an international crisis, when international coalitions dynamically form. In the event of a crisis, whether it is humanitarian relief, natural disaster, combat operations, or terrorist incidents, international coalitions have an immediate need for information. These coalitions are formed with international cooperation, where each participating country offers whatever resources it can muster to support the given crisis. These situations can occur suddenly, simultaneously, and without warning. Often times, participants are coalition partners in one crisis and adversaries in another, raising difficult security issues with respect to information sharing. Our specific interest is in the Dynamic Coalition Problem (DCP), with an emphasis on the information sharing and security risks when coalitions are formed in response to a crisis. This paper defines the DCP and explores its intricate, challenging, and complex information and resource sharing, and security issues, utilizing real-world situations, which are drawn from a military domain.

Categories and Subject Descriptors
C.2.4 [**Computer-Communication Networks**]: Distributed Systems - C*lient/server, distributed applications, distributed databases*. J.7 [**Computers In Other Systems**]: *Command and control, military, process control* . K.6.5 [**Management Of Computing And Information Systems**]: Security and Protection – A*uthentication, insurance, invasive software (e.g., viruses, worms, Trojan horses), physical security, unauthorized access.*

General Terms
Management, Design, Security.

Keywords
Access Control, Distributed Systems, Information Security, Dynamic Coalitions

SACMAT'02, June 3-4, 2002, Monterey, California, USA.

1. INTRODUCTION
Information security was recognized with the advent of the first multi-user computer system for sharing information resources, and as we begin the 21st century, this need has become more significant as countries join together to securely share information at the global level [33]. Information sharing in a secure fashion is a daunting challenge, since we must deal with information content that ranges from the simple to the complex (e.g., intelligence reports, financial information, travel records, citizenship records, military positions and logistical data, map data, etc.) in an interoperable environment that is constantly changing. Recently, numerous mandates have emerged to address information sharing. For example, a vital part of U.S. National Security Strategy states, "whenever possible we must seek to operate alongside alliance or coalition forces, integrating their capabilities and capitalizing on their strengths" [38]. This concept is refined further in our Department of Defense Directives [25] and NATO's interoperability and security concerns [1]. The same information sharing and distributed security concerns have driven many of the U.S. Military's automation plans and initiatives. However, "currently, there is no automated capability for passing command and control information and situational awareness information between nations except by liaison officer, fax, telephone, or loaning equipment" [1]. From the U.S. National Security Strategy to NATO's definition of interoperability, from non-government agencies to their military counterparts, sharing information in a secure manner is recognized as essential.

Our interest for this paper is in secure information sharing that is required in response to a crisis, e.g., natural disaster (earthquake), humanitarian relief (refugee camps), international incidents (terrorism or spy plane), war (Gulf War), or combat operations other than war (Bosnia). Figure 1 depicts five near simultaneous crises in the European Theater. While these crises have different counties involved, there must be information sharing between them to manage resources effectively

throughout the theater of operations. With every crisis solution, there is an accompanying information sharing risk. To handle a crisis, a *coalition* -- an alliance of governmental, military, civilian, and international organizations -- is formed with the primary concern being the most effective way to solve the crisis. The *Dynamic Coalition Problem (DCP)* can be defined as the inherent security, resource, and or information sharing risks that occur as a result of the coalition being formed quickly, yet still finding information and resource sharing a necessity for crisis resolution [36]. The events of September 11 have clearly illustrated the DCP and the difficult issues facing coalitions in information sharing. In the three months following that event, the death toll went from 6,000 to 3,040, and most of the reduction has been traced to "…duplicate reports and confusion in the hours and days immediately following the attack" [CNN.com], which for our purposes, corresponds to multiple databases and inconsistencies in reporting and updating information. The lack of management and sharing of information in this regard clearly illustrates one of the main problems facing a coalition in a crisis. In addition, this information must be securely shared in an easy, efficient, scalable, and reliable way, to facilitate the tasks of the dynamic coalition without compromise and loss of confidentiality. Our focus in this paper is to delineate the critical challenges of DCP with an emphasis on sharing and security, which will be illustrated utilizing real-world scenarios and examples derived from the military domain.

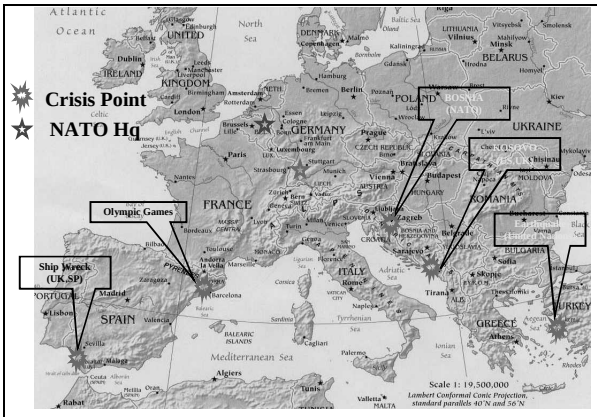

Figure 1. Near Simultaneous Crises.

The work presented herein aligns with many ongoing initiatives to solve information security and interoperability issues. One Department of Defense and NATO effort is the Command Control Systems Interoperability Program (C2SIP) to bring NATO forces together using a database engine that accepts any NATO country formats [1]. The Air Force Research Laboratory in conjunction with Verdian is working on a comprehensive information tagging and release policy called Secure Information Releasability Environment [36]. There are products like e-Portal and Multi-domain Dissemination System, which concentrate on sensitive information access using secure transmission [36]. In addition, there are systems that use firewall technology to create secure network connections between hosts on any unclassified network [22]. All of this work is relevant for different aspects of DCP, but none address the critical issues of federation of resources/users, and the availability and access of resources/information in a secure fashion to support dynamic coalitions.

The remainder of this paper is organized into three sections. In Section 2, we characterize the dynamic coalition problem (DCP), and cite and discuss examples of DCP in civilian and military situations. In Section 3, we focus on the information sharing and security issues relevant to the DCP, including: federation of resources, data integrity, discretionary and mandatory access control, and other critical security issues. In Section 4, we offer a candidate security approach for DCP. Finally, in Section 5, we conclude and discuss ongoing work.

2. THE DYNAMIC COALITION PROBLEM

As discussed in Section 1, coalitions form as the response to a crisis, which is any situation requiring national or international attention as determined by the President of the United States (in our case) or the United Nations (international). Generally, dynamic coalitions of governmental, military, and civilian organizations are formed quickly with minimal regard to the composition of or the political interrelationships of the participants. The Dynamic Coalition Problem (DCP) encompasses all of the varied and wide-ranging issues (i.e., interoperability, sharing, security, extensibility, scalability, etc.) that must be undertaken to form, maintain, and eventually disperse the coalition. The remainder of this section discusses civilian agency involvement in coalitions (Section 2.1), and military considerations via the Global Command and Control System (Section 2.2), raising and exploring the issues that are crucial for supporting information sharing and security for DCP.

2.1. Civilian Organizations

There are many civilian organizations that contribute to the successful resolution of a crisis. These organizations can be government related (agencies, embassies, and bureaus) or non-government (NGOs) and private organizations (PVOs) such as: Local Fire and Police Departments, Doctors Without Borders, FEMA (Federal Emergency Management Agency), NATO, Press Corps (CNN), and the Red Cross. These organizations can handle many situations including: humanitarian relief, nation building, disaster relief, diplomatic problems, refuge situations, etc. Often times, a crisis goes through phases where different agencies take priority roles. For example, in the aftermath of an earthquake, the immediate reaction is to move as many people to safety as possible. This is usually a military mission because the military possess a rapidly deployable lift capability with helicopters and all-terrain vehicles. At a certain point in the crisis, the emphasis shifts towards housing and protecting the displaced personnel (a.k.a. refugees). This responsibility can fall to several organizations, but the International Red Cross in conjunction with a United Nations force, usually provides shelter (tent village), clothing, food and protection to refugees in organized camps. The next concern is sickness and disease caused by unsanitary conditions and lack of clean water. Doctors Without Borders is an international organization that provides doctors and medical supplies to combat the spread of infectious diseases. Water is initially supplied by a bottled water company and delivered by military transport. At the same time, engineering teams are required for construction and plumbing support to these camps in an attempt to provide a

minimal comfort environment, until more permanent facilities can be established or the camp is not needed. Eventually, there is a recovery phase, which includes clean up and rebuilding basic infrastructure to get the region operational.

International NGOs and PVOs usually stay involved in a crisis until the country is self-sufficient and the country's private organizations can take over responsibility. The changes in responsibility and the information sharing requirements to ensure smooth transitions through each phase of a crisis is a difficult management task. Figure 2 depicts a general network architecture of participants (NGOs, PVOs, and military) that need to share information and resources. Figure 2 includes the military command and control systems of five countries. In crisis situations, managing information security is a complex challenge. Since information may be sensitive, and the participants are numerous and constantly changing, and differences in semantics (see Section 3.1.2) need to be overcome.

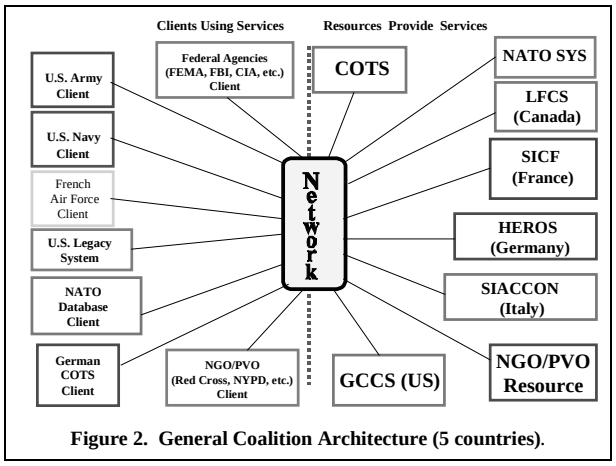

Figure 2. General Coalition Architecture (5 countries).

2.2. Military Involvement: Global Command and Control System (GCCS)

Military forces are often used in crisis situations. In the U. S. Military, information or capabilities sharing is difficult even within our own military services (Army, Navy, Air Force, Marines, and Coast Guard). The problems are exacerbated in a situation where a coalition (possibly disparate national interests) is quickly formed [9]. As coalitions become more complex, the risk of security violations increases, which includes risk to classified intelligence information. U.S. security considerations will need to be maintained and may supercede other coalition needs. Specifically, in some cases, classified information may have to be downgraded temporarily or sanitized for the coalition, but such an act must be done within established security guidelines. The needs of information sharing and security must be balanced in time of crisis. Security mechanisms need to work in *joint* and *combined* environments, where *joint* refers to two or more branches of the Armed Forces (Army, Navy, Air Force, Marines, or Coast Guard) and *combined* is the participation of military from more than one country. Figure 3 depicts the vertical and horizontal lines of communication required to coordinate *joint* crisis operations. Lines of communication include logistic and informational for all aspects of the crisis. Figure 4 depicts the information requirements between multiple countries to support *combined* operations [24].

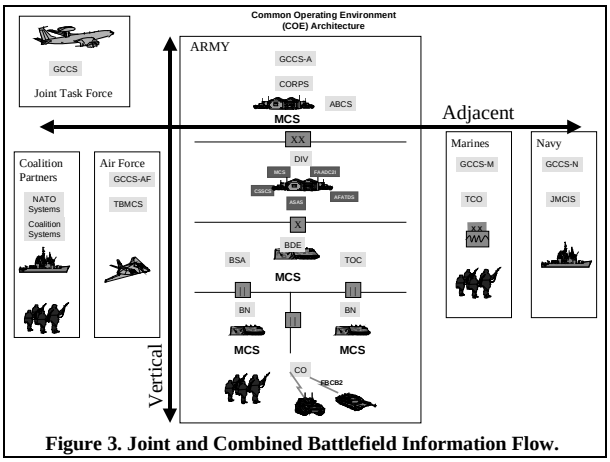

Figure 3. Joint and Combined Battlefield Information Flow.

The information sharing problem is bigger than just classifying information, encrypting data paths, or interoperability; the problem also includes controlling multinational access to resources and adapting to different generations of technology. The current inability to effectively bring international users and their assets (resources) together in a crisis in both an efficient and secure way is very unfortunate, since the actual infrastructure (e.g. localized networks and information resources) can be easily and quickly linked to form an intranet.

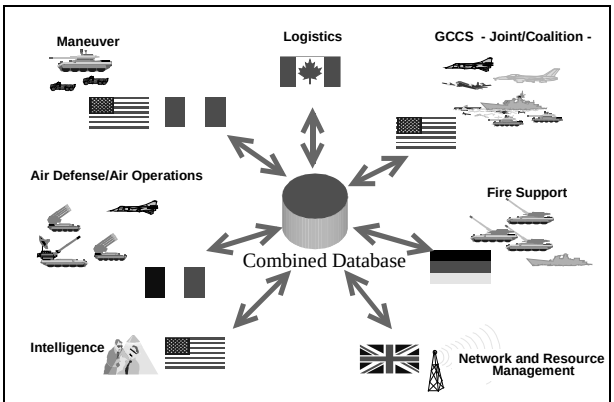

Figure 4. Combined Operations Information Sharing.

Since the U.S. and its military are often called upon in a crisis to supply necessary goods and services, or a unique capability quickly, there must be a system to coordinate this action. The U.S. Military uses the Global Command and Control System (GCCS) to manage such activities. Unfortunately, GCCS does not satisfy all of the needs of a Dynamic Coalition. In a crisis, the flow of critical information and the access to necessary resources is as depicted in Figure 5 [6]. At the present time, GCCS is not designed for the international environment. To be useful internationally, GCCS would need to include a security system that could make it a coalition asset while respecting both coalition and U.S. security policies.

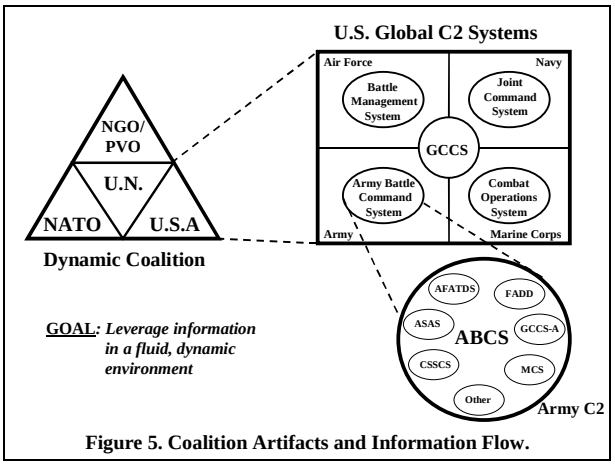

Figure 5. Coalition Artifacts and Information Flow.

GCCS is the automation tool that provides a local U.S. commander operational awareness of the situation (crisis) in near real-time through integrated sets of services as given in Figure 6. GCCS provides information-processing support to planning, mobility, sustainment, and messaging by bringing together 20 separate automated systems in over 625 locations worldwide [19] in a private (physically separate) network. In Figure 6, we present Joint and Component services used to query and change databases or deliver information. The Joint services are used by service members and contain various methods to query the databases of Joint Headquarters and NATO. The Component services allow service members access to individual component (Army, Navy, Air Force, and Marines) command and control systems as depicted in Figure 5. Because GCCS is a U.S. only system on its own private network, security and information sharing issues are different than in a coalition. In order to make the GCCS and other command and control systems acceptable for coalition use, from our analysis, several information sharing and security issues need to be addressed.

Joint Services:	**a.k.a**
Weather	METOC
Video Teleconference	TLCF
Joint Operations Planning and Execution System	JOPES
Common Operational Picture	COP
Transportation Flow Analysis	JFAST
Logistics Planning Tool	LOGSAFE
Defense Message System	DMS
NATO Message System	CRONOS
Component Services:	
Army Battle Command System	ABCS
Air Force Battle Management System	TBMCS
Marine Combat Operations System	TCO
Navy Command System	JMCIS

Figure 6. GCCS Services.

First, we believe that user roles can be a valuable technique to support multiple crisis situations like GCCS. Currently, there are no established roles in GCCS, yet individual service members do play specific roles in a crisis. GCCS users have one user profile that includes all of the permissions that allows access to resources within GCCS as determined by their position, supervisor, and clearance level. In an international coalition, inconsistencies in organizational structure and security clearances will have to be mapped. Currently, users have far more access to resources and information than is required for their positions. Also, a host administrator builds and maintains the user profiles and only receives clearance verification from the security officer. If coalition partners are to share information and resources, there must be a mechanism to restrict access to only necessary information based on a user's role in a crisis. Using static profiles in a crisis, where user requirements are changed or added quickly, is very inappropriate since security is under the control of the host administrator and not the security officer. Using roles can eliminate these profile manipulations by allowing the security officer to change the characteristics of a role or add roles to users dynamically. Then, the host administrator will not need to be involved, since the security officer will have the authority (role permission) to enforce security policy and authorizations. Further, roles can be established dynamically by the security officer to constrain coalition partners to only that information necessary to execute their role. This meets the information security needs of the coalition by using the principle of least privilege.

Second, in analyzing DCP in general and GCCS in particular, it appears that time controllable access for information security is required. Typically, when an individual is assigned an organization, the user profile is provided for an indefinite period of time (much longer than a single crisis). For example, users are often assigned to a crisis for a fixed period of time and allowing access before or after that fixed period of time is a security violation. Recall from Section 2.1, that as the crisis evolves over time, the participants and hence their roles, must also change. Time constraints by role can be used on resources to fix time windows that facilitate database updates or resource allocation. This is the case with GCCS' Joint Operations Planning and Execution System (JOPES). According to policy, Junior Planners must schedule air movements of equipment by air weeks in advance. If an airlift is required inside this window, only Senior Planners can make adjustments, and that is a different role. Currently, these constraints are not automated in JOPES since roles are not clearly established to assign constraints. However, it is clear that the need to constrain access based on time is an important and needed capability.

Third, it seems apparent that in addition to controlling access to information by time, control of actual values that are seen by coalition partners is crucial. For example, the common operational picture (COP) is a capability of the GCCS. COP provides a near real-time mapping of all deployed units worldwide. Figure 7 displays a simulated COP screen capture from a command and control system, where military units are placed onto a digital map, by doctrinal unit symbols [24]. The COP itself takes advantage of inputs from different intelligence sources to map both friendly and enemy positions. Certainly, if one does not have the need to know enemy positions, then there should be constraints on that information. In addition, constraints using map coordinates as parameters, can limit the map view to just the crisis area for a specific user, playing a particular user role. This would limit a non-U.S. coalition partner to viewing force positions only in the area of concern, allowing the user to do his/her job without access to potentially damaging information. Clearly, constraints on resources that focus on allowable values can protect sensitive information while still allowing coalition partners to effectively participate in the crisis.

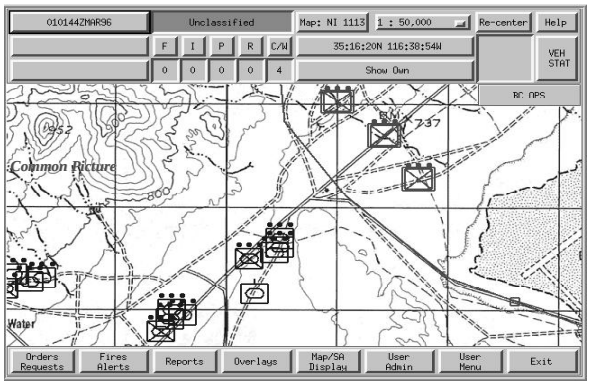

Figure 7. Common Operational Picture.

Finally, in order to manage the GCCS in a joint environment with U.S. forces and multinational partners, the organization and interoperability of coalition assets to yield a distributed environment are a paramount concern. Currently, in multinational crisis situations, there is no dynamic way to effectively bring users and their automation assets (resources) together in an efficient way, as depicted in Figures 2, 3, 4, and 5. Security systems need to allow for quick administration, but still constrain U.S. and non-U.S. users from committing security policy violations. Clearly, users and resources must be federated in a crisis. By using middleware services like JINI or CORBA, resources from coalition partners can be federated with GCCS to make it a more robust and flexible coalition system. In addition, any security solution for DCP must also include an enforcement framework that allows for the management of federated resources and constrain users to security policy limits, limits that also need to be flexible. Our interest in GCCS is to investigate techniques to secure this system in a manner that would make it a coalition asset and respect both coalition and U.S. security policies.

3. INFORMATION SHARING AND SECURITY

Information sharing and security in dynamic coalitions is a complex task, which manifests itself throughout the lifetime of the coalition. The critical issues that arise during a coalition's formation, and in support of its day-to-day management and usage, include, but are not limited to the following:

- Federate groups of users quickly and dynamically in response to a crisis.
- Bring together resources (e.g., COTS, databases, legacy systems, etc.) without modification for usage in support of the crisis.
- Dynamically realize and manage a security policy during simultaneous crises.
- Identify users by their roles to finely tune their access in support of a crisis.
- Authorize, authenticate, and enforce a scalable security policy that can be managed and changed in response to the needs of the coalition.
- Provide a distributed security solution in support of DCP that is portable, extensible, and redundant for survivability.
- Offer robust security policy definition, management, and introspection capabilities that are able to track and monitor system behavior and activities of users.

In this section, we discuss select issues from this list, with a focus on: federating resources from syntactic, semantic, and pragmatic perspectives (Section 3.1); examining data integrity issues in DCP (Section 3.2); exploring discretionary and mandatory access control in support of DCP (Section 3.3); and, briefly reviewing other critical security issues like intrusion detection and cryptography in DCP (Section 3.4).

3.1. Federating Resources

In Figure 8, many of the systems mentioned earlier and represented in Figures 5 and 6 are brought together to illustrate one way that U.S. Military systems can be federated [24]. However, not included in the figures are the many NGOs and PVOs that play important roles in a crisis and also need to be federated, which adds complexity to the coalition forming process. Further complicating the problem is that some of the assets in Figures 2, 3, 4, and 5 contain replicated data in different formats, resulting in data inconsistency that must be addressed for DCP. To focus on these issues, we leverage the concepts of syntax, semantics, and pragmatics [37] to explain information structure, meaning, and usage, respectively. We supply examples from military scenarios that demonstrate the key issues.

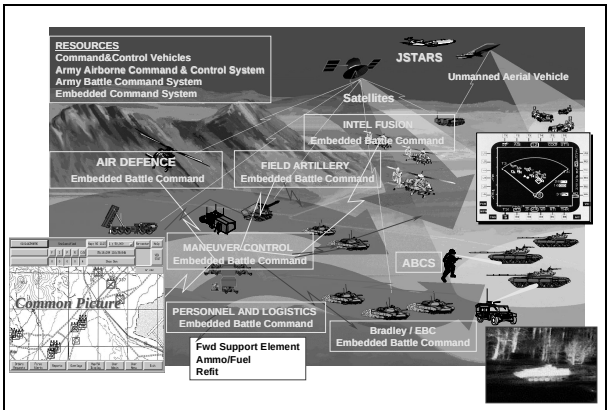

Figure 8. Potential GCCS Federated Resources.

3.1.1. Syntax

For our purposes, syntax refers to the structure and format of the information that is needed to support a coalition. If information is exchanged using an incorrect format or structure, the result could range from a simple error message to a catastrophic action due to the misinterpretation. In information sharing, in order for any data to be processed, strict formats need to be observed, and it is syntax that drives data structure, message formats, and semantics. For example, the U.S. Military communicates using a standard message format comprised of a heading, a text, and an ending section. The heading and ending formats are dictated by the communications systems in use and the text portion of the message is covered by United States Message Text Formats (USMTF) [21]. Since these formats are not currently standard between the different U.S. Armed Forces services, information sharing in joint operations is very difficult, e.g. the U.S. Army and the Marines have different message formats. If the basic

syntax is not observed, a communications systems would not recognize a message as a message.

USMTF is soon to become the standard for use in the U.S. Military. The USMTF program consists of messages whose use is required to exchange certain information. There are 128 different message formats used to gain access to necessary information [21]. These messages are used to update centralized databases, which then make information available to other users. Making USMTF a standard is, in part, a result of the very successful Joint Standardization Program [15], which was used to create the Command and Control Core Data Model. This process took many years and is really a short-lived success story. Over the course of international events, military doctrine has changed to incorporate NATO and multinational coalitions into military and crisis operations. Currently, there are programs such as the Battlefield Interoperability Program, Quadrilateral Interoperability Program [38] and the Command and Control Systems Interoperability Program [7] that attempt to capture necessary information by leveraging message formats. Unfortunately, NATO has far fewer message formats causing another standardization effort driven by syntax. Since Coalition Warfare has become an international interoperability (syntax) effort, with NATO and non-NATO countries, XML has received increasing attention for interoperability of different message formats by using an XML translation [8, 27]. In summary, for dynamic coalitions, the syntax of information must be understood and defined as a key first step to support interoperability across the assets of the coalition.

3.1.2. Semantics

Semantics is, in part, dependent on syntax, but there are semantic constructs that cannot be encoded and recognized syntactically. The semantics of information exchange is a very important interoperability and communication issue. As mentioned in Section 3.1.1, USMTF requires the use of 128 different message formats to request different information. Each message format (syntax) is assigned a semantic interpretation based on the information required to complete the formats. These messages are used for communicating all types of logistical, intelligence, and operational information in a very specific and controlled way in order to coordinate efforts. Each requires specific ways to interpret the message. Potentially, there are basic problems that need to be overcome with semantics. NATO for example, has fewer message formats than USMTF. If there is a different number of message formats, there must be different meanings associated with the different messages. This is not to say there is not a NATO message format that can realize every USMTF, but this cannot be accomplished without some translation. The Command Control Systems Interoperability Program [25] is undertaking the task of translating messages between different message formats.

However, some of the other semantic issues that are problematic involve critical information such as distances, coordinates, classifications, and unit designators. Countries use both Metric and English systems for measurement, so there is an obvious problem if the data given is syntactically correct, but semantically different (miles vs. kilometers). With map coordinates, some systems use magnetic north as a guide and others use true or grid north. It is very common for the U.S. Navy to give position based on degrees longitude and latitude, but it is even more common for a soldier on the ground to give their position in 10 digit grid coordinates (mils). When coordinating indirect fire from ground artillery, naval ships, or aircraft, this is a major information sharing issue (semantic). Of course, one would also imagine the basic spoken and written language differences between coalition partners might lead to semantic issues. There is even a joke amongst our own armed forces about the meaning of the doctrinal term "secure". To the Marines "secure" means blow it up, to the Army "secure" means remove the enemy and occupy, and to the Air Force "secure" means make a down payment. When sharing information, semantic differences must be mapped correctly.

3.1.3. Pragmatics

A detailed understanding of the syntactic structure and the semantic meaning of information for a dynamic coalition drives the pragmatics, in order to clearly quantify and qualify the effective utilization of information. As an example of pragmatics, consider Figures 9 and 10, which depict the information flow in an individual unit's operations center and in an entire division sector respectively [2]. Figure 9 illustrates the different types of messaging systems used and the different files and database snapshots required for facilitating tactical operations. The Tactical Operations Center (TOC) determines information sharing and security needs (who needs what, when and where), and then distributes accordingly. Figure 10 depicts the information flow in an Army Division from the Battalion Level (right side) to the Division Level (left side). Notice that there are a very limited number of connections from higher to lower and left to right and, of course, there are also limits on bandwidth. An Army Division would require communication with dozens of the Tactical Operation Centers as depicted in Figure 9. In order to make information flow efficient, distribution policies must take into consideration the information needed, who needs what information, when and where. These are the pragmatics of information sharing. Consider that Figure 10 depicts only one Army unit that would need to communicate in a joint environment with multiple coalition partners (Figures 2, 3, and 4), and the true complexity of DCP is appreciated.

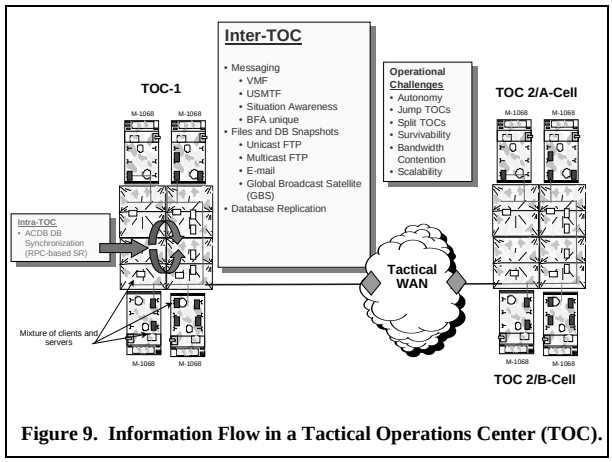

Figure 9. Information Flow in a Tactical Operations Center (TOC).

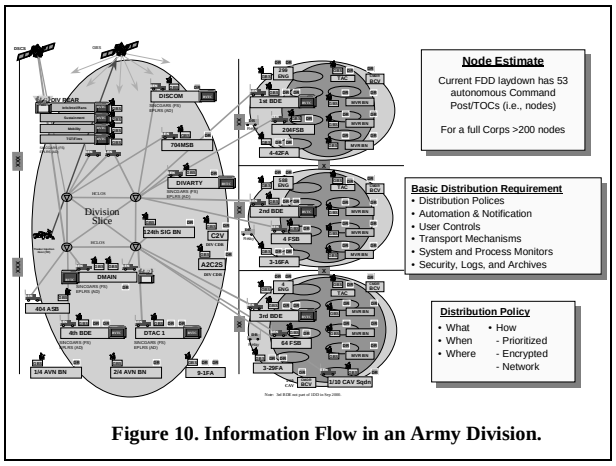

Figure 10. Information Flow in an Army Division.

3.2. Data Integrity

Data integrity is concerned with consistency, accuracy, and reliability. Data integrity is an absolute with military operations. An error in coordinates, a missed time window, or a loss of information could be life threatening. Database errors can be either malicious (security issue) or accidental (integrity issue). Accidental loss of data may result from communication and computer crashes during transmission, concurrent access problems, distribution problems, or logical errors that violate database integrity constraints. Malicious access is more difficult to identify and can cause unauthorized reading, modification, or destruction of data [23]. Given the complexity of coalitions as illustrated in Figures 2-5 and 8-10, and the massive distribution requirements required, accidental problems are guaranteed to occur. Offering redundant communication channels and systems can handle part of this problem. Malicious misuses are not totally preventable, but can be addressed through a comprehensive security policy that limits access to only necessary resources, enforces authentication and authorizations, and provides for consistent backup databases and concurrent updates.

As mentioned earlier (Section 2) dynamic coalitions, are formed quickly and simultaneously. It is possible that partners in one crisis are adversaries in another crisis, which makes information sharing a risk since the potential for misuse is increased. Countries and organizations cannot afford to set up independent information systems for every crisis, and at times, individuals and organizations may have roles in more than one crisis simultaneously (Figure 1). All of these responsibilities (i.e., physical, human, operating systems, and database system) involving data integrity have a significant impact on security in DCP.

3.3. Access Control: DAC and MAC

Successful information security in DCP will require a detailed and intricate security policy that defines what is considered acceptable and unacceptable with respect to access control (what operations are performed on what resource, by who) and information flow (system behavior with information objects) [35]. Authorization, authentication, and, in particular, enforcement mechanisms, will all be an integral part of any coalition. Discretionary and mandatory access control offer many of the capabilities that are needed by coalitions. In the upcoming discussion, we raise the critical issues related to the access control and their relevance to the DCP.

3.3.1. Discretionary Access Control

Discretionary access control (DAC) is a means of restricting access to objects based on the identity of the subject and/or groups to which they belong. The controls are discretionary in that a subject with a certain access permission is capable of passing that permission to any other subject [13]. When information is not sensitive, this type of control is adequate, in that it gives the individual control over distribution and manipulation. In a dynamic coalition, DAC must be carefully administrated to insure that the integrity of information is maintained, and to limit the ability to pass on access restrictions by changing ownership, which is easy to do [32]. For example, when using DAC for DCP, it would be inappropriate for an information owner to give unrestricted access to another user without oversight, since that user could then potentially pass unrestricted access on to another user, without the permission of the original owner. In a coalition, local commanders are not allowed to release information controlled by other owners without the permission of the Defense Intelligence Agency or a Foreign Disclosure officer [36]. Consequently, DAC security policies must be stringently managed and controlled for DCP.

Role-based access control (RBAC), a realization of DAC, regulates a user's access to certain resources based on a *user role*. A user role is a collection of permissions the user needs to accomplish that role. A user may have multiple roles, with each role having a set of permissions. By controlling access using roles and permissions, a security policy can be realized that limits access to the need-to-know information/resources. RBAC has been consistently touted for its ability and utility in support of non-traditional security applications, where flexibility of usage is crucial [34, 39, 40]. Not only does RBAC provide the best flexibility, it is the best for supporting the concept of least privilege, which is a key concern to the military and coalitions. Least privilege allows for access to only that information which is necessary to accomplish one's tasks [18]. In a dynamic coalition, countries are forced to share information and the least privilege is one way to limit access, and consequently, limit potential compromise or misuse. Using RBAC raises some difficult issues when dealing with coalitions such as: who creates the roles? who determines permissions (access)? who assigns users to roles? are there constraints placed on users within those roles? Currently, the U.S. Military has clearly defined crisis roles for U.S. participants; establishing coalition roles are as much a technical issue as a policy/political issue.

There are different RBAC approaches that allow for fine-grained role definition, including our own work [11, 12, 28, 29]. A temporal approach defined in [5] is relevant to DCP due to its changing environment and the shifting of responsibilities. Likewise in [4, 17, 20], the importance of using constraints for identity and authorizations leads to improved granularity on access controls.

3.3.2. Mandatory Access Control

Mandatory access control (MAC) is a means of restricting access to objects based on the sensitivity level (classification) of the information object and the formal authorization level (clearance) of the subject [13]. MAC is required when classified

information is involved. Classified information is national security information that needs special protection against unauthorized exposure [16]. This is not just sensitive information that an organization might want to protect for personnel privacy reasons, this is information that is considered damaging to national interests. There are three classification levels for information: "Top Secret" - expected to cause exceptionally grave damage to national security; "Secret" - expected to cause serious damage; and "Confidential" - expected to cause some damage [16]. When classified information is used, there are very strict access rules based on the Bell-LaPadula Model of enforcement, which establishes a relationship between classifications of objects and clearances of users and the authorized flow of information [3]. The details of these information flow and security requirements are detailed in [14]. These security requirements apply only to U.S. information. Different countries not only have different security requirements, but also apply different security labels to security objects making translation between sensitivity levels a problem for dynamic coalitions. Furthermore, it will be a tedious and difficult task to carefully define the classification levels for coalition partners, particularly since coalitions will likely include past adversaries.

There is a strong likelihood that for coalitions, access control will be accomplished jointly using MAC and DAC. DAC provides discretionality within the boundaries of MAC, and access is only allowed when both DAC and MAC rules are satisfied. Incorporating MAC into RBAC models would allow for the flexibility of RBAC, while observing the strict rules of MAC, providing the best of both approaches in support of DCP. Strict control and flexibility are very different concepts, but can be brought together and prove useful [26, 31]. Data association and aggregation is a problem with any access control mechanism, particularly MAC. A set of data values seen together may have a higher classification value than taken separately (name, unit, and location), a situation likely to occur in coalitions, and there must be security mechanisms sophisticated enough to handle this type of scenario [30].

3.4. Other Critical Security Issues

Our intent in this section is to briefly review a select set of other security issues that must be addressed for DCP. Physical security is always a consideration for information sharing. Physical security as related to information systems can include controlling physical access to equipment, using fiber optic cable instead of coaxial, and establishing controlled procedures for distributing cryptographic keys. While the U.S. maintains private networks to alleviate some of these physical concerns in GCCS, an international coalition dramatically complicates this issue as assets are federated.

Intrusion detection is the ability to detect (not necessarily prevent) unauthorized access or use of resources. This can include network snooping, database manipulation, Trojan Horse activity, and so on. Two concerns of intrusion detection is knowing when information could be corrupt and holding users accountable for their actions. Again, in a distributed coalition environment this is a necessary evil, to insure the proper use and access. Intrusion detection mechanisms include security managers that control access to every resource and log activity, special sensing systems that can detect any change in the physical network continuity (wire taps), and 4-eyes only systems that will allow only access when more than one user is engaged, all of which add complexity to coalitions.

Survivability is concerned with system reliability and accessibility. In a dynamic coalition, information systems go through great turbulence that will cause system outages, which can be devastating in crisis by causing long delays in critical processing or loss of information. One way to improve survivability is to run redundant systems via multiple communication channels, multiple communication mediums, and replicated databases. Clearly, this adds to the complexity of the distributed environment and increases the options for malicious activity within a coalition.

Finally, cryptography is fundamental to establishing security in any environment. In a multinational distributed coalition, cryptography is necessary, but very difficult to achieve. Much of the problem is policy related, since, generally speaking, nations do not share cryptographic material. Public key cryptography is a partial solution to the problem, but also creates a difficult key distribution problem. There has been significant research activity in this area [10, 22].

4. CANDIDATE SECURITY APPROACH

The focus of this section is to discuss a candidate security architecture, model, and enforcement framework to meet the goals of the DCP with a high degree of information assurance. This solution maintains consistency of user roles, clearance and classification levels, and end-user authorizations, to insure that their creation, modification, and deletion will always satisfy the required RBAC/MAC policy.

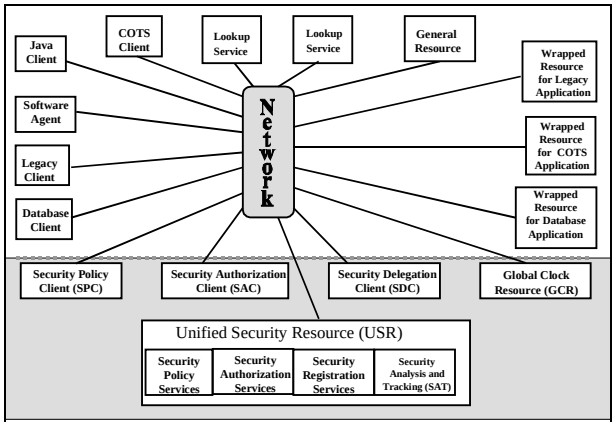

Figure 11: Security Architecture for a Distributed Environment.

Our major emphasis over the past two years has been on the realization of RBAC/MAC security for a distributed resource environment via a constraint-based model and an accompanying enforcement framework [12, 28, 29]. In these works, we have formally defined a security model that includes resources, services, methods, user roles, and signature and time constraints, which supports both RBAC and MAC. Figure 11 depicts our security architecture, which federates users and resources using lookup services. We incorporate a Unified Security Resource (USR) and associated security administrative clients to manage different aspects of security policy (bottom section of Figure 11), which are utilized by clients for registration and dynamic enforcement of security requirements and by resources to

register their services (and methods) for secure access (Figure 12). Our approach has been incorporated into a working prototype using JINI and CORBA as middleware, which also has administrative and management tools to define and monitor the security policy. This architecture is discussed in detail in [12, 28, 29].

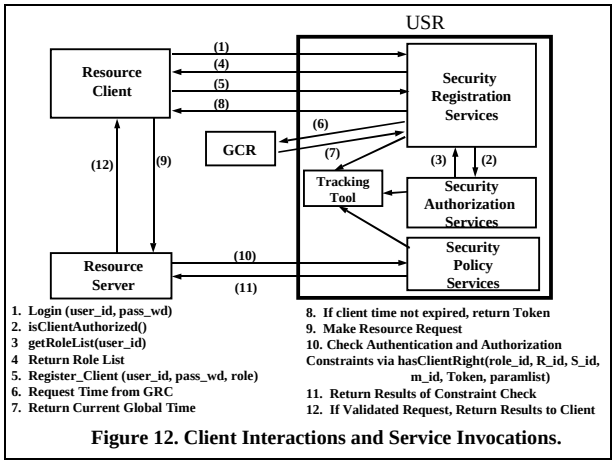

Figure 12. Client Interactions and Service Invocations.

Figure 12 depicts the client interactions and service invocations of our enforcement framework discussed in [12, 28, 29]. This enforcement framework is designed to work with the USR to realize a robust, flexible, and dynamic RBAC/MAC security policy to meet needs of the DCP.

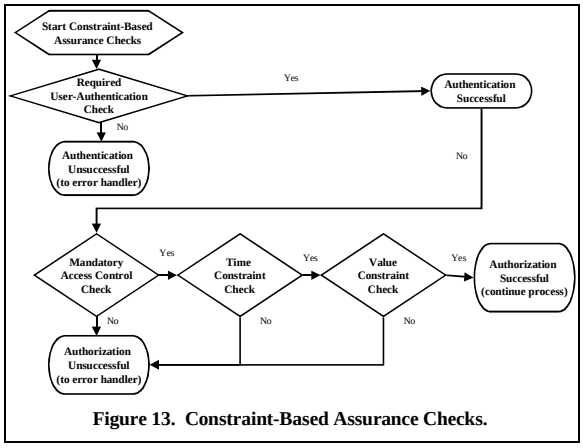

Figure 13. Constraint-Based Assurance Checks.

The processing required by a client joining the distributed environment and attempting to access resources is also given in Figure 12. These steps are detailed in [29] and are part of a comprehensive enforcement framework engineered to verify details of the user, user role and resource at both design and run times for security assurance. Depicted in Figures 12 and 13 are a series of security checks that are all required before an invocation can take place; these checks are summarized in Figure 13 and discussed in detail in [29].

5. CONCLUSIONS AND FUTURE WORK

In this paper, we have examined and explored information sharing and security in dynamic coalitions, which have been formed in response to a national or international crisis. As we have discussed in Section 2, the dynamic coalition problem (DCP) is complex, involving civilian (see Section 2.1) and military (see Section 2.2) organizations whose information and resources must be rapidly federated. Further, based on our knowledge of GCCS, we postulated that coalitions require a number of key capabilities, including: role-based access to information/resources that are dynamically changeable and constraints on information/resources that are time based and value based. In order to transition from GCCS to true global multinational coalitions (see Figures 2, 3, 4, and 5), we discussed the federation of coalition resources and their information from syntactic, semantic, and pragmatic perspectives. In Section 3.1, we examined information consistency for coalitions, with data integrity considered, in Section 3.2. We explored the utility of discretionary and mandatory access control in support of DCP, in Section 3.3, and we briefly reviewed the role of security issues such as survivability and cryptography in Section 3.4. In Section 4, we offered a candidate security approach for DCP by reviewing our existing work on a distributed, constraint-based RBAC/MAC security architecture and enforcement framework. Overall, DCP offers numerous and complex research and experimental challenges in information security.

Ongoing research and prototyping efforts are in a number of different areas. First, designing an extended security model and enforcement framework to support MAC and role delegation; second, there is ongoing research in the ability to define and establish user constraints, which in turn leads to a third area, role deconfliction, which involves both consistency constraints and mutual exclusion. The prototyping effort in support of MAC, role delegation and user constraints, is ongoing, and can be found at: http://www.engr.uconn.edu/~steve/DSEC/dsec.html.

6. REFERENCES

[1] NATO Interoperability from "Advanced Concept Technology Demonstration, Management Plan," PEO C3S HTIO, Fort Monmoth, NJ. 1999.

[2] P. Barr, "ABCS ITDS", MITRE Corporation presentation, NJ, Oct. 1998.

[3] D. Bell and L. LaPadula, "Secure Computer Systems: Mathematical Foundations Model." M74-244, Mitre Corporation, Bedford, Massachusetts, 1975.

[4] E. Bertino, E. Ferrari, and V. Atluri, "The Specification and Enforcement of Authorization Constraints in Workflow Management Systems", *ACM Trans. Info. Syst. Security*, Vol. 2, No. 1, Feb. 1999.

[5] E. Bertino, P. Bonatti, and E. Ferrari, "TRBAC: A Temporal Role-Based Access Control Model, " *Proc. of the Fifth ACM Workshop on Role-based Access Control*, Berlin Germany, July 2000.

[6] S. Boutelle and C. Pizzutelli, "Army Battle Command System," *Army RD&A*, Sept./Oct. 1998.

[7] Prepared by PEO C3S HTIO, "Command, Control, Communications, and Computers Interoperability for Coalition Warfare, Advanced Concept Technology Demonstration, Management Plan," Ver. 1.2, March 1999.

[8] M. Cokus, "XML-MTF, A Military XML Vocabulary," The MITRE Corporation, 2001.

[9] DARPA ITO Sponsored Research, Spring, Kohout, Yates, "2000 Project Summary, Flexible Coalition Policies for Secure Information Sharing," Verdian-PSR, 2000.

[10] J. Baras, V. Gligor, and R. Poovendran, "Integrated Security Services for Dynamic Coalition Management," DARPA ACT Program, March 2001.

[11] S. Demurjian and T.C. Ting, "Towards a Definitive Paradigm for Security in Object-Oriented Systems and Applications, " *Journal of Computer Security*, Vol. 5, No. 4, 1997.

[12] S. Demurjian, T.C. Ting, H. Ren, J. Balthazar, C. Phillips, and P. Barr, "A User Role-Based Security Model for a Distributed Environment," *Research Advances in Database and Information Systems Security*, J. Therrien (ed.), Kluwer, 2001.

[13] Department of Defense Directive 5200.28-STD, "Department of Defense Trusted Computer Systems Evaluation Criteria," December 1985, Authorized by DoD Directive 5200.28, Dec. 1972.

[14] Department of Defense Directive 5200.28, "Security Requirements for Automated Information Systems (AIS)," March 1988.

[15] Department of Defense Directive 8320.1-M-1, Department of Defense, "Data Standardization Procedures," March 1996. http://jcs.mil/htdocs/teinfo/software/8320.html

[16] R. Reagan, Executive Order 12356, "National Security Information," The White House, Apr. 1982.

[17] D. Ferrailo, "The Role Control Center: An Implementation of Role-Based Access Control on Identity-Based Systems," NIST White Paper, 2000.

[18] D. Ferraiolo, "An Argument For The Role-Based Access Control Model," *Proc. of Sixth ACM Symp. on Access Control Models and Technologies*, Chantilly, VA, USA, May 2001.

[19] Joint Operational Support Center. "Global Command and Control Center," DISA, 1999. http://gccs.disa.mil/gccs/

[20] T. Jaeger "On the Increasing Importance of Constraints, " *Proc. of the Fourth ACM Workshop on Role-Based Access Control*, Fairfax, VA, USA, Oct. 1999.

[21] *JIEO Handbook 9000*, Chapter One, "General Instructions," Joint Information Exchange Operations, Department of Defense Handbook, March 2000.

[22] D. Kindred and K. Djahandari, "Adaptive Network Defense, Dynamic Virtual Private Network," Networks Associates Technology, Inc., NAI Labs, 2001, see http://www.pgp.com/research/nailabs/adaptives-network/dynamic-virtual.asp.

[23] H. Korth and A. Silberschatz, *Database Systems Concepts*, "Security and Integrity", Chap. 13, McGraw-Hill, 1986.

[24] S. Levine, "Army Modernization: Digitization and Transformation Overview," briefing at Pentagon, April 2000.

[25] C. Milster, M. Parish, G. Le Fevre, "Taking Digitization to Our Allies, " *Army RD&A*, Sep-Oct 1998.

[26] S. Osborn, R. Sandhu, and Q. Munawer, "Configuring Role-Based Access Control To Enforce Mandatory And Discretionary Access Control Policies," *ACM Trans. Info. Syst. Security*, Vol. 3, No. 2, 2000.

[27] W. Peach, "Message Text Formats-A Solution to the Problem of Interoperability," *Journal of Battlefield Technology*, Vol. 2, March 1999.

[28] C. Phillips, S. Demurjian, and T.C. Ting, "Security Engineering for Roles and Resources in a Distributed Environment", *in Proc. of the 3rd Annual Information Systems Security Engineering Conf.*, March 2002.

[29] C. Phillips, S. Demurjian, and T.C. Ting, "Toward Information Assurance in Dynamic Coalitions", Comp. Sci. and Engr. Dept., Univ. of Conn. (CSE-TR-02-3), February 2002.

[30] P. Samarati, "Access Control: Policies, Models, Architectures, and Mechanisms," *FOSAD*, Italy, Sept. 2000.

[31] R. Sandhu, "Lattice-Based Access Control Models," *Computer Journal*, Vol. 26, Nov. 1993.

[32] R. Sandu and P. Samarati. "Access Control: Principles and Practice." *IEEE Communications Magazine*, Vol. 32, No.9, Sept. 1994.

[33] R. Sandu, "Role-Based Access Control", *Advances in Computer Science*, Vol. 48. M. Zerkowitz (ed.), Academic Press, 1998.

[34] R. Sandu and Q. Munawer, "The ARBAC99 Model for Administrative Roles," *Proc. of 15th Annual Computer Security Applications Conf.*, Phoenix, AZ, Dec. 1999.

[35] F. Schneider, "Enforceable Security Policies," *ACM Trans. Info. Syst. Security*, Vol. 3, No.1, Feb. 2000.

[36] S. Spring and D. Gormley, "Information Sharing for Dynamic Coalitions," VPSR Report 2836, Verdian Pacific-Sierra Research, Dec. 2000.

[37] R. Tennent, *Principals of Programming Languages*, Prentice Hall, London, 1981.

[38] Quotation from the National Military Strategy, "C4I For Coalition Warfare, Command and Control Systems Interoperability Program," Army Digitization Office, 1999.

[39] T.C. Ting, "A User-Role Based Data Security Approach," *Database Security: Status and Prospects*, C. Landwehr (ed.), North-Holland, 1988.

[40] T.C. Ting, "Application Information Security Semantics: A Case of Mental Health Delivery," *Database Security, III: Stauts and Prospects*, D. Spooner and C. Landwehr (eds.), North-Holland, 1990.