AFRL-RH-WP-TR-2014-0073

Survey of Collaboration Technologies in Multi-level Security Environments

Mark S. Crabtree
Ball Aerospace & Technologies Corporation

John D. Ianni
Air Force 711 HPW/RHCV

April 2014

Interim Report

STINFO COPY

BATTLESPACE VISUALIZATION BRANCH
AIR FORCE RESEARCH LABORATORY
HUMAN EFFECTIVENESS DIRECTORATE
711th HUMAN PERFORMANCE WING
AIR FORCE MATERIEL COMMAND
WRIGHT-PATTERSON AIR FORCE BASE, OH 45433-7334

Notice and Signature Page

AFRL-RH-WP-TR-2014-0073 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

//signed//
JOHN D. IANNI
Program Manager
Battlespace Visualization Branch

//signed//
JEFFREY L. CRAIG
Chief, Battlespace Visualization Branch
Warfighter Interface Division

//signed//
WILLIAM E. RUSSELL
Chief, Warfighter Interface Division
Human Effectiveness Directorate

REPORT DOCUMENTATION PAGE

Form Approved
OMB NO. 0704-0188

1. REPORT DATE *(DD-MM-YY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
28-04-14	Interim	**1 Sep 2013 - 28 Feb 2014**

4. TITLE AND SUBTITLE

Survey of Collaboration Technologies in Multi-level Security Environments

5a. CONTRACT NUMBER	FA8650-08-D-6801/0050
5b. GRANT NUMBER	N/A
5c. PROGRAM ELEMENT NUMBER	0602202F
5d. PROJECT NUMBER	5329
5e. TASK NUMBER	11
5f. WORK UNIT NUMBER	53291103/H08J

6. AUTHOR(S)

Mark S. Crabtree, Ball Aerospace & Technologies Corp.
John D. Ianni, Air Force, 711 HPW/RHCV

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Ball Aerospace & Technologies Corp
Systems Engineering Solutions
2875 Presidential Drive, Suite 180
Fairborn, OH 45324-6269

Air Force Research Laboratory
711 HPW/RHCV
2255 H Street
Wright-Patterson AFB, OH 45433

8. PERFORMING ORGANIZATION REPORT NUMBER

AFRL-RH-WP-TR-2014-0073

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory
Human Effectiveness Directorate
711th Human Performance Wing
Air Force Materiel Command
Wright-Patterson Air Force Base, OH 45433-7022

10. SPONSORING/MONITORING AGENCY ACRONYM(S)

711th HPW/RHCV

11. SPONSORING/MONITORING AGENCY REPORT NUMBER(S)

N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT

Distribution A: Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES

88 ABW Cleared 07/16/2014; 88ABW-2014-3418. Report contains color.

14. ABSTRACT (Maximum 200 words)

This report surveys technologies and methodologies that foster collaboration in multilevel security (MLS) environments. One of the unique challenges of national defense is the handling of highly sensitive and compartmentalized information. In this era of WikiLeaks and other compromises to our nation's investments in security, the rules for information access are understandably not easing. Most who have proper access have the right intentions yet these information security measures, at best, slow their progress if not stifle it in some cases. Teamwork in particular suffers. Therefore, as part of the Air Force Research Laboratory (AFRL)-National Reconnaissance Office (NRO) Experiment (ANX), AFRL's Human Effectiveness Directorate (RH) was asked to determine the state-of-the-art in MLS collaboration technologies and make recommendations. The goal was not to find ways to circumvent operational security, but rather to promote collaboration without compromise.

15. SUBJECT TERMS

Collaboration, multilevel security, teamwork, decision making

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Mr. John Ianni
Unclassified	Unclassified	Unclassified	SAR	100	19b. TELEPHONE NUMBER

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18

TABLE OF CONTENTS

SUMMARY

This report surveys technologies and methodologies that foster collaboration in multilevel security (MLS) environments. One of the unique challenges of national defense is the handling of highly sensitive and compartmentalized information. In this era of WikiLeaks and other compromises to our nation's investments in security, the rules for information access are understandably not easing. Most who have proper access have the right intentions yet these information security measures, at best, slow their progress if not stifle it in some cases. Teamwork in particular suffers. Therefore, as part of the Air Force Research Laboratory (AFRL)-National Reconnaissance Office (NRO) Experiment (ANX), AFRL's Human Effectiveness Directorate (RH) was asked to determine the state-of-the-art in MLS collaboration technologies and make recommendations. The goal was not to find ways to circumvent operational security, but rather to promote collaboration without compromise.

INTRODUCTION

Collaboration is a critical aspect of any enterprise. If teams are not able to work together effectively, productivity suffers (Tierney & Steele, 2012). Today's collaborative environments require that individuals with different roles, skills, and clearances work together—typically across one or more computer networks—to fulfill mission requirements. Tough security measures, while critical, can have an effect on an enterprise's productivity be it in national defense or a corporation protecting intellectual property. Balancing information security and access has long been a challenge for designers of information security systems (Dorsett, 2005).

Many processes, procedures, network architectures, and other security measures have been implemented specifically to keep classified information out of unauthorized hands (Hinton, 2006). While strong information security can be critical, less is known about methodologies and tools that enhance productivity in these environments and across the security levels. Uncovering these is the purpose of this paper.

Before we started our investigation of collaboration tools, we felt it was important to understand how organizations protect their information without delving too deeply into specific classified practices. A common technique used to protect sensitive information is multilevel security (MLS). This is the cornerstone of the safeguarding process where information is classified at various levels so that only those individuals, organizations, and facilities with proper security clearances and the need for the information can access it. These levels allow a wider group to access the less sensitive information with only highly vetted individuals allowed to access the highest security levels.

MLS can mean different things to different people but a common definition is *a scheme for classifying information into security levels to ensure only those appropriately cleared with a need to know should receive access* (Accenture, 2009; Irvine & Levin, 2002).[1] MLS is also thought of as a capability and, indeed, we needed to consider these aspects as well (Bell, 2005).

MLS poses many challenges for organizations including:

(1) Keeping the information from "leaking" outside the network.

(2) Making information available only to those with proper credentials (i.e., security clearances) within the network.

[1] The authors of this paper do not claim to be experts in MLS but it was apparent that some consider it a security environment while others a capability. This paper actually must consider both the environment and the capabilities that enable MLS.

(3) Preventing individuals from receiving "pieces" of classified information that when assembled have a higher classification than the recipient is authorized for.

(4) Maintaining appropriate security while making sure that individuals who are authorized to access information can do so in a timely fashion without significantly adding to their workload.

(5) Facilitating collaboration and sharing of information so that work groups achieve a common understanding of mission purpose, plan, goals, requirements, and task assignments.[2]

Addressing these challenges often results in a conflicted solution for securing and sharing information (e.g., Lanahan, 2011; Cianciolo, LaVoie, Foltz, & Pierce, 2009; Kim, Zhu, Smari, & McQuay, 2006). While much effort is spent to protect vital information, it is sometimes denied to critical members of collaborative teams because it is classified at a higher level than their clearances allow them to access. The result is that not everyone in the team is working with the same knowledge of mission objectives and current status. Apparently, this is such a common problem in many MLS environments that it is viewed as "systemic."[3]

Security across a network

MLS systems are used extensively throughout the DoD and other agencies, as well as most large enterprises with networked operations. Networking, while challenging for security, brings benefits such as better situation awareness through high-speed information sharing, improved command and control (C2) functions (planning and decision making) through facilitated collaboration, and cost reduction from improved efficiency of operations. These benefits help make corporations more competitive, and position military organizations to more effectively and rapidly execute missions for achieving specific objectives (Brodbeck, Mazza, & Lalanne, 2009).

Suites of software applications run on complex network structures to facilitate gathering and sharing of information, and collaboration among users. Significant increases in situation awareness can be achieved as distributed collaborative environments expand to accommodate additional active participants – human and machine, domestic and international. Because of the high value of information available on these networks and

[2] Collaboration is generally more than just "sharing" information. It may also involve command and control activities (i.e., coordination of team effort by assigning tasks, distributing workload, and monitoring progress), development of shared mental models, team problem solving, team decision-making, multi-point data acquisition, and distributed learning.

[3] "There is a systemic problem with data sharing. Part of it stems from ignorance about information technology—what it can and cannot do—which causes those responsible for determining sharing policy to err on the side of conservatism." --Bryant (2007), p 77.

the potential damage that could result if the information were leaked to adversaries or competitors, organizations install MLS safeguards to protect it.

This report was written from the perspective that MLS technology is applied in networked environments where there is a group of individuals working together as a team, and often as a distributed team, with a common mission. A huge amount of past research on team performance is applicable in this situation (e.g., Mesmer-Magnus & DeChurch, 2009; Salas, Guthrie, Wilson-Donnelly, Priest, & Burke, 2005; Guzzo & Dickson, 1996).

In short, research has demonstrated that team decision-making and overall team effectiveness may be significantly impaired when information cannot be shared among team members. For optimal performance, it is highly important that the team has an accurate shared mental model of their mission, each other's tasks, roles, and capabilities, who has what information (i.e., information that is needed for performing their tasks), difficulties their teammates may be having performing their tasks, and other factors that constitute an accurate shared mental model (e.g., Kennedy, 2011; Banks & Millward, 2007; Sperling, Pritchett, Estrada, & Adam, 2006; Greenberg & Dickelman, 2000).

The inability to share information among team members has been well documented in recent years such as during international responses to natural disasters (e.g., hurricane Katrina and the earthquake in Haiti) (e.g., Patel & Olson, 2012; Eovito, 2006). Multinational defense exercises requiring collaboration and coordination of land, air, sea, and space resources in particular have significant challenges because not all parties have proper clearances to receive all pertinent and necessary information (IMISAS Project, 2012; Eovito, 2006; Treece, 1999). Given such instances of collaboration difficulties, as well as other undocumented similar instances that have reportedly occurred in military operations centers, there is sufficient reason to believe that the challenges imposed by the MLS issue are not insignificant.

When teammates have differing mental models due to suboptimal information sharing decision making can suffer greatly (Weil, Carley, Deisner, Freeman, & Cooke, 2006). This can also increase mental workload, decision making time, and frustration. Especially in high tempo operations, a common human response for overcoming obstacles such as these is to devise and implement unauthorized "workarounds" that allow the warfighters to maintain productivity and achieve the team objective. But in the MLS environment, such implementations could inadvertently jeopardize information security (Macklin & Jenket, 2005).

Effective and permissible solutions to the MLS productivity problem could improve interoperability among agencies; international or coalitional sharing of data; and sharing of information within a distributed team (Hamilton, Dumay, & Scott, 2008). While individuals working within an operations center are usually all cleared at a high level, this is not always the case. Even within highly secure facilities, there is often a need for small work-groups to have special clearances for specific projects.

Given the critical importance of an accurate "shared" or "common" mental model for effective team performance and decision-making, we sought to find methods and approaches to support collaboration among individuals in MLS teams despite obstacles posed by critically important security measures.

The Research Objective

A goal of this research project was to identify *human-centered* approaches for aiding and supporting MLS collaboration while maintaining security and integrity of classified information and data. Collaboration included chat, messaging, imagery, and voice, as well as shared electronic blackboards and whiteboards. The approach was to conduct an extensive literature search for recent publications related to this topic and, where possible, supplement the search with inputs from individuals familiar with MLS issues in military and commercial operations centers. To assist with the research, the Human Effectiveness Directorate enlisted the help of Ball Aerospace personnel through the Warfighter Interface Research and Technology Operation contract, FA8650-08-D-6801, Task Order 50. This report documents the research approach and the results.

METHODS, ASSUMPTIONS, AND PROCEDURES

Initially, the research focused narrowly on identifying the means and mechanisms for team members to collaborate in MLS environments via 3-D simulations such as JVIEW, NASA WorldWind, Analytic Graphics, Inc. Satellite/Systems Toolkit (STK), and/or shared blackboards. After several discussions, it was agreed that the goal of this project would be better served by broadening the research to identify general human-centered solutions to facilitate collaboration and the development of shared or team mental models in MLS environments. Several topics were then identified as being relevant to this search. These were:

- Human-computer interfaces that support sharing of information in secure collaborative environments. These would include workplace human factors and ergonomics concepts that support both collaboration and information security.

- Effects of MLS technologies and methods on team performance, workload, situation awareness, and decision-making in collaborative environments.
- Visualizations to facilitate collaboration in MLS environments. These include visualization concepts to support a common operating picture (COP) where some are denied access to certain information. The research, if any exists, should ultimately be applicable to the development of a display or a "visualization" that can enhance the team's shared mental model and collaboration among team members.
- Lessons learned from situations where operators were unable to complete critical tasks because of security impediments.
- Security "workarounds" devised by operators so they can perform critical tasks. Information about this item was envisioned to be especially difficult to find because of the sensitivity of the topic.
- Ways that members of a distributed team form common or shared mental models of situations (e.g., mission progress, status of assets, what a particular group under surveillance is doing, etc.) when not all team members have the same information.

Search Terms and Resources

To attempt to address the above topics, many different sets of search terms were generated and tested in a wide range of search engines and databases. Basic examples are provided in Table 1 below. This is my no means a complete list of terms used because the basic terms were modified in real-time as each database was searched and the "hits" were evaluated. The resources used for the searches included the databases available through the D'Azzo Research Library at Wright Patterson Air Force Base, the online technical research capabilities provided by Ball Aerospace, and numerous databases available to the public through the internet. Of particular importance to this search were the databases available through:

- DTIC – http://www.dtic.mil/dtic/
- Engineering Village – http://www.engineeringvillage.com/home.url?acw=
- Google Scholar – http://scholar.google.com/
- IEEE Xplore® Digital Library – http://ieeexplore.ieee.org/Xplore/home.jsp
- ScienceDirect – http://www.sciencedirect.com/
- Science.gov – http://www.science.gov/

- SCIRUS – http://www.scirus.com/ (scheduled to be retired before this report is published)

TABLE 1. EXAMPLES OF TERMS USED IN LITERATURE SEARCH.

Search Term Example	No. of hits	Nature of Articles (from very brief skim of abstracts)
collaboration AND (JVIEW OR WORLDWIND OR STK)	245	General discussions of the collaboration tools, their applications, development, and features. No discussion of specific collaboration problems and their effect on performance.
collaboration AND "3D World" OR "3D environment"	136	Descriptions of the development and use of 3D World concepts to improve data understanding.
"problems in collaboration" OR "collaboration problems" OR "challenges in collaboration" OR "collaboration challenges" OR "difficulties in collaboration" OR "collaboration difficulties"	92	Fundamental principles of team or work group collaboration. Good basics.
"collaboration tools" OR "collaborative tools" AND "human factors issues" OR "usability issues" AND space OR satellite	45	Some good discussions of the barriers to use of and the problems associated with collaborative tools.
satellite AND space AND "problems in collaboration" OR "collaboration problems" OR "challenges in collaboration" OR "collaboration challenges" OR "difficulties in collaboration" OR "collaboration difficulties"	53	Wide range of reports. General discussions of development of improved collaborative technology but few human-centered design requirements.
"collaboration tools" OR "collaborative tools" AND "security classification"	204	Several relevant discussions of collaborative tools requirements. A few articles are cited in this report.
"interface design" AND "collaboration" AND "MLS" OR "multilevel security"	21	Reports not as relevant as expected.

“collaboration tools” AND "different security clearances"	4	Articles were more concerned with high level policy than operational application.
security AND text OR chat OR collaboration AND "automated classification"	5	Highly technical articles; some points were mentioned in this report.
How do collaborators with different security clearances share information?	>1000	Too many articles to review in detail.
“shared mental model” OR "team mental model" AND visualization AND "incomplete information” OR “missing information”	63	This search provided useful information. Some articles are cited in this report.
“classified information” AND "collaboration tools"	749	DTIC was the only database searched. Some articles are cited in this report.

Given their background in human performance, researchers involved in this project were already aware of the vast literature on team behavior and performance, and especially the importance of shared mental models and collaboration among team members to promote better team SA and decision-making. Therefore, the decision was made not to review that particular literature or include the articles in Appendix C. (Some relevant literature regarding team performance and shared mental models is cited in specific instances where it intersects with MLS topics.)

Both Air Force and contractor personnel acknowledged the potential difficulties of executing this research project. An envisioned difficulty was the possibility that very limited information exists in the open literature describing:

(1) Human factors considerations in the design of MLS systems and other security measures for use with collaborative tools in classified environments.
(2) Situations where human operators are unable to complete tasks because of security impediments.
(3) Incidents of human operators devising and deploying security workarounds so they can perform their tasks and execute their missions.

Information about the last item was envisioned to be especially difficult to find because of the sensitivity of the topic. Despite these potential obstacles, the decision was made to press on with the research and report any relevant findings.

The search turned up more than 1200 articles which were downloaded and reviewed. Fewer than 100 were sufficiently related to this project to be read and included in Appendix C. The next section gives a brief summary of the findings and discussion.

RESULTS AND DISCUSSION

Information technology (IT) security specialists often suggest that the MLS problem can be solved through both hardware and software technologies such as multiple firewalls, isolated or layered networks, and secure logins. Because a priority of MLS is to prevent collaborators with different clearances from sharing information, the usual approach to developing an MLS plan is to design for utmost information security with less emphasis on understanding user tasks or information sharing requirements. A quick, initial search of the literature turned up very few examples of MLS technology having been designed and implemented specifically to address the information sharing needs of the collaborators, although one might consider work performed by the Naval Postgraduate School an exception (Eovito, 2006). Generally, the emphasis appears to be mainly hardware and software solutions for protecting classified information. The few "human-centric" solutions are discussed later in this section. There was little discussion found of MLS implementation within JVIEW, STK, and WorldWind, although apparently STK can operate within the MLS environment (Gavin, 2010).

Current Methods to Facilitate Collaboration in MLS Environments

Many of the articles reviewed discussed concepts to improve collaboration through high-level policy change, network design and software tools (JWFC Doctrine Pam 5, 2004), and approaches to improve general interoperability[4]. Only a few publications (e.g., Cloutier & McComb, 2012) mentioned the need to determine the human-centric collaboration requirements through methods such as cognitive task analyses or users' needs analyses.[5,6]

[4] Not long ago, "interoperability" referred mainly to the ability of multiple agencies using two-way radios to operate on common radio frequencies using the same modes. The term is now sometimes used to refer to the ability of two or more individuals or organizations to access the same computer networks for chat, text messaging, and file sharing.

[5] According to Fernandez Vazquez, Pastor Acosta, Brown, Reid, & Spirito (2012), "Engineers focus on technical aspects of information sharing networks, and often do not take into consideration the social, organizational, and cultural systems of use" (p 431).

[6] However, one specific collaboration tool—Chat—which is the real-time transmission of text messages, is considered so important in today's military C3 environment that Navy personnel have completed one or more needs analyses and have been successful in instituting a DoD-wide MLS chat policy. Chat can be an effective synchronous or asynchronous method to communicate and collaborate in high-paced military operations (Eovito, 2006).

Some of the concepts mentioned below have actually been implemented while others have been proposed, or are still being evaluated. They are primarily listed below in this order: technological solutions, policy solutions, and human-centered solutions.

Technological Solutions

1. Use of multiple networks

Most articles that describe technology solutions for the MLS environment focus on layered and isolated networks with only information of specified security levels allowed on each network (e.g., General Dynamics, 2012). Information of a higher level is generally forbidden on the network. In some cases, a network is established for each security level. Only individuals with the necessary clearances can log onto the appropriate network. There may be considerable cost associated with establishing and maintaining multiple networks with differing security requirements. An annoying usability issue occurs when users need information that is not available on the network they are logged into. Even though the user may have the necessary clearance to access the needed information on another network, special and often cumbersome procedures may be required to access it. This can make the sharing of information in a timely fashion quite difficult (General Dynamics, 2012; Raytheon, 2010; O'Malley, 2009; Winjum & Berg, 2008; Hinton, 2006).

2. Use of chat rooms cleared at the appropriate levels

Chat rooms requiring specific clearance levels for entry are established for collaboration. Controls such as biometric signatures could be established so that each chat room permits entry only of those individuals with clearances of the appropriate level. All discussions involving classified data take place only in the chat room with the appropriate clearance level. A benefit of chat rooms is that there would be some assurance that everyone in the "room" has the appropriate clearance, so there would be less need to monitor and assess every term or phrase. This approach eliminates the use of (or does not eliminate the multi-level security issues associated with) email and voice communications. If chat rooms were implemented along with the metadata approach mentioned elsewhere, all digital message traffic could be recorded, categorized, and perhaps analyzed for content fairly easily. Unless biometric signatures are employed, the same security issues with regard to account sharing (discussed below) remain (Duley, Flynn, Abich, Drabik, Szalma, & Hancock, 2007; Eovito, 2006; Hinton, 2006).

3. More secure login procedures

The suggestion has been made that users sometimes "share" accounts in classified facilities (e.g., Eovito, 2006, p 18; Spannuth, 2002; Andrews, Packard, Alberts, White, & Crane, 2000, p 29). One reason for this is that the login process is often time consuming, and the work tempo may demand immediate responses from those individuals just coming on duty. Thus, it is easier/faster for the arriving individual to continue using the account of the individual going off duty than to initiate a new login. While this is against regulations, policies, and procedures for numerous reasons, a very important concern in the current context is that not every potential user is cleared to the same level, and someone with a lower level clearance could be using the account of someone who holds a higher level clearance. Therefore, meta-data attached to chat messages or other digital communications from an individual using another's account could provide the recipient with incorrect clearance information, and the recipient could respond with information of a higher classification than the sender is allowed to receive (Zhang, Brodsky, Swarup, & Jajodia, 2008).

A possible solution to this problem is the use of biometrics or biometric signatures for login, or for continuous authentication (Ikehara & Crosby, 2010). This is a very active research and development area, and many products have been implemented and tested including fingerprint readers, retinal scanners, facial recognition, and speaker recognition (Gray, 2010). It is somewhat surprising that wider-scale use of biometrics has not been observed. One could assume that their use would speed-up up the login process immensely, but the lack of trust in today's biometric systems (Chen, Pearson, & Vamvakas, 2002) is an obstacle that has to be overcome before widespread implementation can occur (Kleist, 2007).

The goal of stricter login procedures is to prevent users from sharing accounts, and thereby accessing networks and chat sessions that are classified at a level higher than the user is permitted to access. Thus, this is not an approach to facilitate collaboration, but in a sense, to prevent it. Many ways have been proposed to create more secure login procedures. Possibly a *combination* of biometric signature, password, and Common Access Card (CAC) would accomplish this goal without impeding access to information by legitimate users.

4. Use of meta-data

A few articles briefly mentioned the use of meta-data attached to "chunks" of real data as a means to achieve multi-level security. This was mentioned in the literature in the context of chat data. The meta-data could be attached to a data "packet" (which would have to be defined). The meta-information "tag" would contain the security classification of each message (or of the facility or operation from which it was sent), identification of

the sender and the facility, identification of the intended recipient, and perhaps even the security clearance of the recipient (e.g., Mysore, 2013; Nguyen, Levin, & Irvine, 2005). (Some meta-data information might be used only during later review of archived chat sessions, as in an after-action review.) Automatic controls would be put in place to prevent tagged data from being seen by an individual with an inappropriate security clearance (Clark, Levin, Irvine, & Shifflett, 2009). Similar techniques could be applied to digital voice communications, the transmission of digital photos and digital full-motion video (FMV), and email messages.

5. Automatic Classification of Data

The notion here is that the classification level of *each* communication is determined individually in real-time (Brown & Charlebois, 2010; Benali, Ubéda, & Legrand, 2008). This avoids one potential sharing problem that occurs when *all* communications coming from a facility about a specific event is designated Secret, Top Secret, etc. "Blanket" designations such as this often totally prevent classified information from getting to the collaborators who really need it (Zhang, Brodsky, Swarup, & Jajodia, 2008). Some work has been done with automatic classification of messages based on specific words occurring in specific contexts. There was no mention of how successful this approach has been when implemented in an operational setting. This could be a topic for a future focused literature search.

6. Use of Various Software Tools

Various software tools have been developed to facilitate collaboration within the MLS environment. Reviews of these concepts, tools, methods, hardware, etc., are provided in several documents (e.g., Ong, Nguyen, & Irvine, 2008; Duley, Flynn, Abich, Drabik, Szalma, & Hancock, 2007; CINCI 21, 2003; Spivey, 2002). Several articles review collaboration tools, and the developers describe some of them on their websites (e.g., General Dynamics, 2012; Raytheon, 2010; 2013; Accenture, 2010; 2009). A review focused specifically on the human-centric aspects of available collaboration tools, their features, and their capabilities could be very useful for addressing the goal of the project.

Policy and Agreements

1. Agreements

In some cases, having a priori agreements with other organizations regarding what can and cannot be shared can facilitate collaboration. These agreements would be established long before collaboration attempts begin. Security levels would be known and agreed on by all parties. Even the clearances of participating individuals could be known. The formal networks to be used, what information is contained on each

network, and the security requirements for access to each network would be known to all participants. Such agreements are sometimes used for international collaborations (Fernandez Vazquez, Pastor Acosta, Brown, Reid, & Spirito, 2012). Some countries have no experience with MLS and can't deal with it. Singer also says the greatest need is help visualizing intelligence knowledge instead of writing documents or preparing presentations. Their products would become a multimedia human friendly "transfer of knowledge." Admiral Singer says they try to make all shared information only Secret. Nothing above. (Ackerman, 2007)

2. Overarching Policy

Several papers discuss the need for a DoD-wide MLS policy that provides some standardization to the technical approaches being used. A common complaint is that every organization uses different tools and architectures, which make interoperability, collaboration, and data sharing more difficult. Because of the popularity and utility of chat as a primary means for collaboration, earlier articles strongly encourage the development of a common DoD policy with regard to MLS and specific mediums such as chat and chat rooms. This has actually been addressed in a recent DoD Standards document (DoD Manual 5200.01, Vol. 2, 2012), but it is not clear if it has gone far enough in addressing chat issues.

3. Classify Sparingly, or Declassify

There is a concern expressed throughout the literature that data/information is "overclassified" (e.g., Dawson, De Capitani di Vimercati, Lincoln, & Samarati, 2002). It is often classified at a too high level, and in many cases, doesn't need to be classified at all (Libicki, Jackson, Frelinger, Lachman, Ip, & Kalra, 2010). Rather than relying on personnel clearances and MLS technologies to limit access to classified data, centers might attempt to declassify information and intelligence (Thomas, Cuppens-Boulahia, & Cuppens, 2011) , or when possible, not classify it at all. As mentioned elsewhere in this report, a highly experienced SME suggested that much classified data--at least in the intelligence community--is classified because the source of the data and the method of collection cannot be divulged. In some cases, the data itself is not classified, may even be available open source (see Bryant, 2007, p 74), and should be declassified (see Thomas, Cuppens-Boulahia, & Cuppens, 2011). Reducing the amount of information that is classified, or classifying it at a lower level, would make it more easily disseminated to public safety and private sector partners (see United States Department of Justice, 2007, p 49). Because so much useful information is unclassified, orienting users toward open source information causes the sharing within MLS problem to go away (Ackerman, 2007).

4. Uniform Clearances

One of the most common techniques used to avoid sharing of information with individuals with inappropriate security clearances is to make sure that all personnel in a facility or participating in an operation are cleared to the same level. SMEs indicated that members of teams or groups working within operations centers mostly work at the same clearance level. So sharing information is not normally a problem. Of course, this does not help with the need to share information with individuals outside the center who may have different clearances. Also, the concept of "uniform clearances" does not apply internationally because standards and requirements for each security clearance level differ from country to country (Vazquez, Acosta, Spirito, Brown, & Reid, 2012).

Human-Centered Approaches

1. In Essence, One-Way "Collaboration"

A primary reason for collaboration to occur in an MLS environment is to share information so that a common mental model can form among all team members. Failure of the model to develop can occur when not everyone on the team has the same security clearance, and some are denied vital information that can affect their decision-making. A partial means for circumventing this problem is to allow higher cleared personnel to have the ability to see what lower cleared personnel are talking about, especially through chat. This allows the higher level personnel to know what the lower level personnel actually know, and to see what sort of shared mental model they have developed. In this way, the higher level personnel can guide the lower level personnel, or through various other means, try to prevent them from making bad decisions.[7] Systems have been designed to assist those with high security clearances in knowing what those with lower clearances are saying on secure websites at the appropriate security level. Of course, those with lower level clearances would not see the information being shared among those with higher level clearances (Ong, Nguyen, & Irvine, 2008).

Sometimes analysts with higher level clearances will try to guide lower level people's decisions or conclusions based on the greater knowledge and understanding that the higher level person has but can't share because of security classification. The higher level person may come up with questions to "steer" the lower level person's thinking, and to give the impression, "Trust me; I am experienced; I've been there before." Or, the

[7] Decision-making with only partial information is a very interesting area of current research. Although the emphasis of the current project is two-way sharing of information, another search topic that could provide useful insight to the design of tools to support collaboration in the MLS environment is decision-making with only partial information derived from one-way communication.

higher level person may asked questions to encourage the lower level person to think of more possibilities or outcomes, which may cause him or her to dig deeper into the available data, or look for more data. According to some SMEs, this is by far the most common interaction between people with different clearances within the intelligence community.

2. Human-Centered Analog to Layered Networks

SMEs indicated that analysis of intelligence data is done at whatever level it needs to be done. In operations centers there is often no need for higher security level personnel to provide information to people at the lower security level. Apparently, the viewpoint exists that people at the lower level are more operational and don't need the higher level information. "They just do what they're told to do" seems to be a common notion. In essence, they are operating within a security "layer" that provides them with the information that supervisors feel they need.

3. Reports for Different Security Levels

An organization producing intelligence information may perform actual collections at the higher security level, and then release a report at a lower level if a plausible source for the information exists at the lower level. Protection of the source of information is often the reason for the higher level of classification. Therefore, the existence of a plausible source at a lower level of classification (or even in open source) means that the actual source, whose identify needs to be protected at a higher level, is no longer an issue.

It is usually very important to protect both the sources and the methods of data collection. So, it may be okay in some instances to share data if the source and method of collection are not known, or are removed from the rest of the data. The source and collection method often determine the higher classification. The information itself may not be classified at the higher level. Of course, someone is responsible for determining the proper classification of the information. The possibility of automatic classification was discussed elsewhere in this document.

4. Confirm security clearance

Another behavioral technique that may contribute to collaboration is simply to confirm the other party's clearance. According to SMEs, there have been instances where people needing to work together assumed they had different clearances when in fact they were all cleared to the same level, or they all had clearances at or above the level needed for the information to be shared. If they had confirmed their clearances, they could have shared the information. Of course, confirming security clearances is especially important where there are compartmentalized conference rooms.

5. Traditional “Manual” Means for Sharing Classified Information

Technique #1: An individual or a group with a high-level clearance decides what minimal information is needed by the individuals with lower-level clearances to carry out their mission. Then the individual or group reviews the higher-level information, extracts what is needed, re-works it in some way so that it is no longer classified at the higher level, and then disseminates it (through whatever means) to those who need it.

Technique #2: “Sneakernet” refers to the sharing of information between computers that are not connected to the same network, or otherwise cannot access the same information, when the computer users need the same information. This sort of sharing is usually done by copying information to a CD in one computer, and carrying the disc to another computer (Smith, 2001). This action could result in an inadvertent security breach, so care must be taken to properly safeguard the information and make certain that all users have the proper clearances. If the user of the receiving computer is cleared at a lower level than the information being received, then manual technique #1 above must be employed. An obvious potential problem with this technique is that it is not “real-time” and could result in delays in decision-making.

General Issues Associated With Multi-Level Security

The current effort was intended mainly as a survey of tools and methods for facilitating collaboration specifically within MLS environments. The significance of the operational impact of MLS issues mentioned above cannot be determined from the literature search and review performed in this effort. Likewise the success of many of the solutions that address these issues is largely unknown. To answer these specific questions, a focused research effort would be required. However, some of the difficulties encountered in developing and implementing tools and methods to support collaboration in MLS environments *were* suggested by a few of the reviewed articles. These obstacles include the following:

Cost

Establishing multi-level security is a complex problem. Obviously, the complexity of the security requirements grows as the facility’s complexity increases. Top notch IT security specialists are in high demand and are costly (see Smith, 2001, for a discussion of cost of MLS systems). Some environments are so complex that months of system characterization are required before a security plan can be developed or modified (Saydjari, 2004). Also, in some cases, implementing multi-level security may require some “down time” of certain network resources. This may not be possible if events are happening that require continuous collaboration.

Lack of systematic process for determining users' needs

Much care is needed in performing the system analysis required for designing an MLS system. Few articles were found that mention the use of cognitive task analyses (CTAs) or other knowledge elicitation tools in the design of MLS systems, but such tools are likely to be essential for making sure that system designs afford collaborators access to the information they need when they need it. It's critical to understand user information requirements and how users employ collaboration tools (Adams & Sasse, 1999). While there is a general notion that usage information should be incorporated into the design of systems, there is often no formalized attempt to characterize user requirements (e.g., Mancuso, Strang, Funke, & Finomore, 2014; Erdogan, Anumba, Bouchlaghem, & Nielsen, 2008).

Lack of over-arching architecture and/or a "General Approach"

It is likely that a different multi-level security plan has to be developed for each MLS facility. It is rare that two major collaborative facilities have sufficiently similar requirements to permit a common solution. Each solution is likely to be specific to the site/installation/organization. Apparently, this is why several articles shared the common theme that an over-arching *network architecture* for implementing multi-level security does not exist (e.g., Andrews, Packard, Alberts, White, & Crane, 2000). Likewise, there does not seem to be an over-arching *policy* for multi-level security within government-operated collaborative environments. Because literature addressing the issue of policy was not specifically sought, reviewed articles relating to policy were not necessarily current. If this is a topic of interest, newer articles on network architectures and overarching MLS policies should be sought and reviewed.

SMEs' Views of MLS Human-Centric Issues

In the course of performing this research, two significant human factors issues related to MLS were discussed with SMEs. One is the real-time decision-making requirements of operators sitting in an operations center viewing and responding to chat and other data from various sources, and having to determine what can be shared and with whom in real-time. The other problem, which was mentioned elsewhere in this report, is the possible sharing of accounts.

The SMEs were highly experienced security professionals. Two had been managers within major intelligence operations centers (one military and the other civilian); two had various military backgrounds with considerable intelligence operations center

experience; and one was a civilian security officer. Here are some of their relevant comments made during interviews. Some are quotes and others are paraphrased:

"The sharing of classified information with individuals without proper clearances *cannot*, *does not* happen. Period."

"Individuals with higher level clearances may release reports to individuals with lower level clearances on an 'as needed' basis, but pieces of information that require the reports to be classified at a higher level will have been removed or redacted. Oftentimes, only the source of the information and how it was collected are the elements that require the report to be classified at the higher level. If these elements are removed (and usually they aren't necessary in order for action to be taken), then the rest of the information or report may not be classified at the higher level."

"Individuals with higher level clearances who must collaborate with individuals with lower level clearances may ask questions to stimulate the thinking of the individuals with the lower level clearance. This is done not to pass on classified information, but to cause the individual with the lower level clearance to continue 'digging' for more information, or looking for alternative explanations that could be better descriptions of the true situation."

"Information such as the size of our forces, the equipment that we're using, the whereabouts of troops and equipment, and the schedule that we're adhering too are often the only elements that are classified at the higher level. With this information removed, reports can sometimes be provided to lower-cleared personnel."

"Team members mostly work at the same clearance level. So sharing information is not normally a problem." [However, multinational teams may present a different kind of MLS problem because—for example—a Top Secret clearance in one country does not mean the same thing in another.]

"It would be a very rare situation for someone to leave their shift without logging out, thus allowing another person with a different clearance to use their account. It is conceivable that this could happen in a high tempo situation, but it would be the rare exception to the rule."

There is no question that difficulties in collaborating and deciding on a course of action do occur in MLS environments. There does not seem to be established means for dealing with them. They usually get resolved, but not always in a timely manner. Situations have been observed where individuals with different clearances could not

agree on an action because the individual(s) with the higher clearance had more information and could not share it with the others. These individuals were seen having private meetings that apparently resolved the issue(s), but how they were resolved is not known. There is no reason to believe that security was compromised.

Multi-Level Security Specifically Involving Geospatial Simulations

In the literature reviewed there are few discussions of multi-level security in regards to geospatial simulations such as JVIEW and World Wind. Several articles mention STK and multi-level security in the same context, but the papers that have been reviewed in detail did not indicate that MLS is a feature of STK, although STK is capable of running in an MLS environment (Gavin, 2010).

If little or no work has been done to implement MLS within such simulations, and if there is a desire to design such implementation, then several additional steps are required:

1. Develop an understanding of the collaboration scenarios or situations where MLS is a concern.
2. Understand the collaborators' tasks, information requirements, how they perform their roles, and where MLS breaches are likely to occur. A starting point might be to perform a CTA on users of JVIEW, STK, and/or World Wind; or, make use of an existing CTA if the necessary data are available.
3. Develop an understanding of the architectures of JVIEW, STK, World Wind, and other geospatial simulations, and the network architectures on which they run, so that a plan for integrating MLS can be developed.

CONCLUSIONS & RECOMMENDATIONS

Based on the literature reviewed and the finding that little has been done in the MLS domain to assist team performance and decision making through improved collaboration, a human-centered approach to improve shared mental development among team members is posited. The approach is drawn from a combination of existing technologies and some technologies that seem feasible, but may not have been developed yet. Key features of the technologies to be incorporated are described below:

- Automatic classification. Despite the fact that classification decisions can be subjective, "computerized" classification could allow a more standardized, and possibly faster, supplement to these decisions (Bolloju, 1999). This feature could include a type of wizard capability that would provide recommendations as an alternative to more autonomous methods. In any case a more uniform classification process could promote more detailed classifications where small chunks of data could be appropriately classified (e.g., within a paragraph). When performed strictly by a human, such activity is often too time-consuming. With an autonomous or semi-autonomous classification approach, a smart-agent operating on a network could monitor all data at all times and constantly update the security status of every data packet. This would provide the user with a near-real-time data classification update. Promising research on automatic data classification is described in the literature (e.g., Benali, Ubéda, & Legrand, 2008; Brown & Charlebois, 2010; Gehres, Louthan, Singleton, & Hale, 2010; Hennessy, Lauer, Zunic, Gerber, & Nelson (2009).

- Automatic declassification. Similar to the above, as specific information becomes declassified, markings could be automatically updated thereby making information available sooner to a wider population. If sensitive information is found to be available in open source, it could be declassified, linked to the open source locations, or other actions taken. Rapid computerized determination if the data to be shared is available as "open source" should permit faster dissemination.

- Continuous biometric monitoring for identity authentication. Envisioned here is a system to conduct continuous facial recognition, or retina or iris scans, to make certain that the appropriately cleared person is the only one accessing or viewing the classified data (Ikehara & Crosby, 2010). This would essentially eliminate the problem of account sharing.

- Extensive use of metadata. All data packets on the classified network would contain classification level, originator and date of origin, and who has read or seen the information/data. Using this scheme, there would be no question about the classification level of any data—chat, text, imagery, telemetry, etc. at any time. Also, this forms the foundation for a system that presents only the data that is appropriate to each individual's security clearance—a concept described below.

- New visualization concepts. The notion is that a display, which is envisioned as a "common operating picture" or COP, would be developed to show only that information for which the user is cleared to see (using the metadata concept above). Individuals with higher level clearances would see more information on their workstation displays than would individuals with lower level clearances. If security regulations permit, individuals with information missing from their displays would be informed, and they would also be shown which individuals in the team have that information (i.e., their displays would indicate which information is missing, and who has it). A brief notional development of the concept is provided in Appendix A. This visualization concept should be particularly useful for high-level managers and commanders because they could see who has what knowledge across the entire operation. Personnel with lower level clearances could take some comfort in knowing that at least certain individuals in the team or organization have the knowledge they think is critical to the mission, but can't access.

  Since a COP of this type is believed to be a new concept, considerable research would be required during its development and evaluation. At least two kinds of research are envisioned. One would be research into intra-team dynamics and team performance when some members are shown only part of the needed information, while other individuals have more information (Richter, Hirst, van Knippenberg, & Baer, 2012). The other would be research into display designs for the COP itself. This research would involve determining the best means to display a notice of missing information (and who has that information) that is compliant with security regulations, and that enhances the user's situation awareness regarding what information is missing and who has it. Evaluations would be needed to assess team performance with and without the new information visualization.

- Smart decision-making aids. Intelligent agents could be especially beneficial for individuals with lower clearance levels. These agents would have access to all data, regardless of security level, and could feed appropriate information to the cleared individual as he/she needs it. The agent could determine which portions of the data are open source and thereby provide more information to the user than he/she would otherwise be able to access. Perhaps the agent could also contribute to the

decision-making process in other ways, but this notion would have to be developed (Hutchins & Kendall, 2011; Fan, McNeese, & Yen, 2010). A preliminary development of the concept is provided in Appendix B.

- Probability-based scenarios. Consistent with what one of the SMEs mentioned regarding prompting individuals to keep probing the data for additional hypotheses, smart agents could do the same thing but in a different way. The big difference is that in the SME's description, a human with a higher-level clearance has access to the higher-classified information that the lower-level person does not have access to. Therefore, the higher clearance level person can use the higher classified data to guide the lower level person into generating more hypotheses to test. By contrast, the smart agent envisioned here would have access only to the same information as the lower-level user, but would help the user generate alternative hypotheses based on historically probable outcomes given the current context and the data that both the user and the smart-agent have access to. The goal would be stimulate the user's thought processes to generate more hypotheses and outcomes so that he/she would "dig deeper" and do more research, data collection, and analysis before making a decision (Convertino, G., Wu, A., Zhang, X., Ganoe, C.H., Hoffman, B., & Carroll, J.M., 2008).

Appendix C is a table of articles that were either used in this report, or that are relevant to this report. Some of those articles discuss tools, procedures, methods, etc., that have been designed to support MLS in collaborative environments. The notions put forth in this report were derived mainly from ideas presented in those articles. Further pursuit of these notions would require a much more thorough review and assessment of the technologies described than the current effort was intended to accomplish.

In addition to partial solutions described in the body of this report and its Appendices, alternative approaches for solving the collaboration in MLS environments problem doubtlessly can be conceptualized. Perhaps the ideas mentioned here will at least serve as "food for thought."

REFERENCES

[1] Accenture (2009). Increasing Capability to Both Protect and Share Information: A Complete Security Approach to Achieve High Performance in Defense and Intelligence. http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Defense_Security_Approach_for_High_Performance_in_Defense_and_Intelligence.pdf.

[2] Accenture (2010). Multi-level security common operating picture. http://blogs.agi.com/agi/2010/09/23/maintaining-a-synchronized-common-operating-picture-between-networks-of-varying-security-levels/.

[3] Ackerman, R.K. (2007) *Terrorism*, Technology Drive Pacific Intelligence Needs. *Signal*, Oct. 2007, 62, *2*.

[4] Adam, A. & Sasse, M.A. (1999). Users are not the enemy: Why users compromise security mechanisms and how to take remedial measures. *Communications of The ACM,* 42(*12)*, 40-46.

[5] Andrews, A., Packard, S., Alberts, C., White, T., & Crane, L. (2000) Defense Healthcare Information Assurance (DHIAP) Phase I Composite Evaluation Report. ATI IPS TR 00-02, Contract No. DAMD17-99-C-9001, U.S. Army Medical Research and Materiel Command, Fort Detrick, Frederick, Maryland 21702-5012.

[6] AGI (2013). STK10. http://www.agi.com/default.aspx

[7] Banks, A. P., & Millward, L. J. (2007). Differentiating knowledge in teams: The effect of shared declarative and procedural knowledge on team performance. *Group Dynamics: Theory, Research, and Practice,* 11, 95–106.

[8] Bell, D. E., (2005). Looking Back at the Bell-La Padula Model. Proceedings of the 2005 Annual Computer Security Applications Conference. http://www.acsac.org/2005/papers/Bell.pdf.

[9] Benali, F., Ubéda, S., & Legrand, V. (2008). Collaborative approach to automatic classification of heterogeneous information security. *The Second International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2008*. August 25-31, 2008, Cap Esterel, France.

[10] Bolloju, N. (1999). Decision model formulation of subjective classification problem-solving knowledge using a neuro-fuzzy classifier and its effectiveness*, International Journal of Approximate Reasoning,* 21, *3*, 197–213.

[11] Brodbeck, D., Mazza, R., & Lalanne, D. (2009). Interactive Visualization - A Survey. D. Lalanne and J. Kohlas (Eds.): *Human Machine Interaction,* LNCS 5440, pp. 27–46. Springer-Verlag: Berlin Heidelberg.

[12] Brown, J.D. & Charlebois, D. (2010). Security classification using automated learning (SCALE): Optimizing statistical natural language processing techniques to assign security labels to unstructured text. Defence R&D Canada – Ottawa Technical Memorandum DRDC Ottawa TM 2010-215, December 2010.

[13] Bryant, S.A. (2007) Geospatial Informational Security Risks and Concerns of the United States Air Force Geobase Program. AFIT/GEM/ENV/07-M1, Department of the Air Force, Air University, *Air Force Institute of Technology*, Wright-Patterson Air Force Base, Ohio.

[14] Chen, L., Pearson, S., & Vamvakas, A. (2002). A trusted biometric system. Trusted E-Services Laboratory, HP Laboratories Bristol, HPL-2002-185, July 15th, 2002.

[15] Cianciolo, A. T., LaVoie, N., Foltz, P., & Pierce, L. G. (2009). *Augmented performance environment for enhancing interagency coordination in stability, security, transition, and reconstruction (SSTR) operations* (Tech. Rep. 1246). Arlington, VA: U. S. Army Research Institute for the Behavioral and Social Sciences.

[16] CINCI 21 (2003). Joint Military Utility Assessment for the CINC 21 Advanced Concept Technology Demonstration. Technical Report 1899, SSC SAN DIEGO, San Diego, California 92152-5001 July 2003.

[17] Clark, P.C., Levin, T.E., Irvine, C.E., & Shifflett, D.J. (2009). DNS and Multilevel Secure Networks: Architectures and Recommendations. NPS-CS-09-004. Naval Postgraduate School, Center for Information Systems Security Studies and Research (CISR), 1411 Cunningham Road, Monterey, CA 93943.

[18] Cloutier, R. & McComb, S. (2012). Prototype of a Graphical CONOPS (Concept of Operations) Development Environment for Agile Systems Engineering. Final Technical Report SERC-2012-TR-030, Systems Engineering Research Center, Stevens Institute of Technology, 1 Castle Point on Hudson, Hoboken, NJ 07030.

[19] Convertino, G., Wu, A., Zhang, X., Ganoe, C.H., Hoffman, B., and Carroll, J.M. (2008). Designing Group Annotations and Process Visualizations for Role-Based Collaboration. College of Information Sciences and Technology, The Pennsylvania State University, University Park, PA, 16802, 197-206.

[20] Deputy Director Joint Staff, Joint and Coalition Warfighting (JCF); Smith, K. (Attn.): Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Project. Final Report. Joint Development, Solutions Evaluation Division, 116 Lakeview Parkway, Suffolk, VA: February, 2012.

[21] Dorsett, D.J. (2005). Tsunami Information Sharing in the Wake of Destruction. *Joint Force Quarterly: JFQ 39* (Fourth Quarter 2005): 12-18.

[22] Duley, A.R., Flynn, J., Abich, J., Drabik, H., Szalma, J., & Hancock, P. (2007). Collaborative technologies and their effect on operator workload in BMC2 domains. AFRL-HE-WP-TR-2007-0054. Air Force Research Laboratory, Human Effectiveness Directorate, Warfighter Interface Division, Collaborative Interfaces Branch, Wright-Patterson AFB OH 45433.

[23] Eovito, B. A. (2006). The Impact of Synchronous Text-Based Chat on Military Command and Control. 2006 Command and Control Research and Technology Symposium (2006 CCRTS): The State and the Art of the Practice. Naval Postgraduate School, 1 University Circle, Monterey, CA 93943.

[24] Erdogan, B., Anumba, C., Bouchlaghem, D., and Nielsen, Y. (2008). Collaboration environments for construction: implementation case studies. *J. Manage. Eng.*, 24(4), 234–244.

[25] Fan, X., McNeese, M., and Yen, J. (2010). NDM-Based Cognitive Agents for Supporting Decision Making Teams. *Human-Computer Interaction,* 25(*3*): 195 — 234.

[26] Fernandez Vazquez, D., Pastor Acosta, O., Brown, S., Reid, E., Spirito, C. (2012). Conceptual framework for cyber defense information sharing within trust relationships. 4th International Conference on Cyber Conflict (CYCON), 5-8 June 2012.

[27] Gavin, N. (2010). STK in a multi-level security environment. Presented at the 3rd Conference on Artificial General Intelligence (AGI), Mar. 5 2010 – Mar. 8, 2010, Lugano, Switzerland.

[28] General Dynamics (2012). Trusted network environment (TNE) security. General Dynamics C4 Systems, 8220 East Roosevelt Street, M/D R7229Scottsdale, AZ 85257

[29] Greenberg, J. D. & Dickelman, G. J. (2000), Distributed Cognition: A Foundation for Performance Support. *Perf. Improv,* 39: 18–24. doi: 10.1002/pfi.4140390608

[30] Gray, S.C. (2010). *Leveraging naval riverine forces to achieve information superiority in stability operations*. Master's Thesis. Naval Postgraduate School, Monterey, CA 93943-5000.

[31] Guzzo, Richard A. & Marcus W. Dickson. 1996. "Teams in Organizations: Recent Research on Performance and Effectiveness". *Annual Review of Psychology,* 47:307-338.

[32] Hall, D.L.; McNeese, M.; Yen, J.; & Seif El-Nasr, M. (2006) A Three Pronged Approach for Improved Data Understanding: 3-D Visualization, Use of Gaming Techniques, and Intelligent Advisory Agents. In *Visualising Network Information* (pp. 8-1 – 8-12). Meeting Proceedings, RTO-MP-IST-063, Paper 8. Neuilly-sur-Seine, France: RTO. Available from: http://www.rto.nato.int/abstracts.asp.

[33] Hamilton, A., Dumay, J., & Scott, J. (2008). Transnational Information Sharing Coalition (TISC) JCTD. Project Sponsors: EUCOM, AFRICOM, SOUTHCOM, DISA, OSD-AS&C, & OSD-NII.

[34] Hennessy, S.D., Lauer, G.D., Zunic, N., Gerber, B., & Nelson, A.C. (2009). Data-centric security: Integrating data privacy and data security*. IBM J. Res. & Dev*., Vol. 53, No. 2, Paper 2, 2009.

[35] Hinton, G.D. (2006). Multiple independent levels of security: The changing face of range information management in the 21st century. *ITEA Journal*, June/July 2006, 11-12.

[36] Hutchins, S.G. & Kendall, T. (2011) The Role of Cognition in Team Collaboration During Complex Problem Solving. Chapter 5 in *Informed by Knowledge: Expert*

Performance in Complex Situations, edited by Kathleen L. Mosier, Ute M. Fischer. Taylor & Francis: NY, NY 10016.

[37] Ikehara, C.S. & Crosby, M.E. (2010). Physiological measures used for identification of cognitive states and continuous authentication. *CHI 2010*, April 10–15, Atlanta, Georgia.

[38] Irvine, C. E. & Levin, T. (2002). A Cautionary Note Regarding the Data Integrity Capacity of Certain Secure Systems, in *Integrity, Internal Control and Security in Information Systems*, ed. M. Gertz, E. Guldentops, L. Strous, Kluwer Academic Publishers, Norwell, MA, pp 3-25.

[39] Joint Warfighting Center (JWFC). (2004). The Joint Warfighting Center Joint Doctrine Series Pamphlet 5. Joint Warfighting Center, United States Joint Forces Command, 116 Lake View Parkway, Suffolk, VA 23435-2697.

[40] JWFC Doctrine Pam 5. (2004). The Joint Warfighting Center Joint Doctrine Series: Operational Implications of the Collaborative Information Environment (CIE). Joint Warfighting Center United States Joint Forces Command 116 Lake View Parkway Suffolk, VA 23435-2697, 1 Jun 2004.

[41] Kennedy, D. M. (2011). Team creative processes: The importance of complementary and shared mental models. *Proceedings of the 44th Hawaii International Conference on System Sciences,* 1-10.

[42] Kim, S. Y., Zhu, J., Smari, W., & McQuay, W. (2006). Security and access control for a human-centric collaborative commerce system. *The 2006 International Symposium on Collaborative Technologies and Systems*, Las Vegas, NV, USA, May 14-17, 2006, pp. 429 - 439.

[43] Kleist, V.F. (2007). Building technologically based online trust: can the biometrics industry deliver the online trust silver bullet? *Information Systems Management*, 24(*4*).

[44] Libicki, Jackson, Frelinger, Lachman, Ip, & Kalra (2010) *"What Should Be Classified? A Framework with Application to the Global Force Management Data Initiative"*, Rand National Defense Research Institute Prepared for the Joint Staff J-8. Library of Congress Control Number: 201094085, ISBN: 978-0-8330-5001-4.

[45] Macklin, T. & Jenket, P. (2005). *Achieving cross-domain collaboration in heterogeneous environments.* Paper presented at the RTO IST Symposium on

"Coalition C4ISR Architectures and Information Exchange Capabilities", held in The Hague, The Netherlands, 27-28 September 2004, and published in RTO-MP-IST-042.

[46] Mancuso, V.F., Strang, A.J., Funke, G.J., & Finomore, V. (2014). *Human factors of cyber attacks: a framework for human-centered research.* Paper presented at the 2014 International Annual Meeting of the Human Factors and Ergonomics Society, Chicago, Illinois, October 27-31. Published in *Proceedings*.

[47] Messmer-Magnus, J.R. & DeChurch, L.A. (2009). Information sharing and team performance: a meta-analysis. Journal of Applied Psychology, 94, 2, 535-546.

[48] Moore, J.A. (2002). JView: an information visualization paradigm. *Proc. SPIE*, Vol. 4716, 367-374. In *Enabling Technologies for Simulation Science VI*, Alex F. Sisti; Dawn A. Trevisani (Eds.).

[49] Mysore, P. (2013). Analysis of data provenance across various applications. Presented to the faculty of the Department of Computer Science, California State University, Sacramento**.** Submitted in partial satisfaction of the requirements for the degree of Master of Science in Computer Science, Spring 2013.

[50] NASA (2013). World Wind Java SDK. http://worldwind.arc.nasa.gov/java/

[51] Nguyen, T.D., Levin, T.E., & Irvine, C.E. (2005). MYSEA Testbed. *Proceedings of the 2005 IEEE Workshop on Information Assurance and Security*, United States Military Academy, West Point, NY

[52] O'Malley, S.A. Free to flow: A paradigm shift for multi-level security data exchange. AU/ACSC/O'MALLEY/2009. Air Command and Staff College, Air University, Maxwell Air Force Base, Alabama.

[53] Ong, K. L., Nguyen, T. and Irvine, C. (2008). Implementation of a multilevel wiki for cross-domain collaboration. *3rd International Conference on Information Warfare and Security (ICIW 2008),* Omaha, Nebraska, pp. 293-304.

[54] Patel, D. M., & Olson, S. (2012). Information Sharing and Collaboration: Applications to Integrated Biosurveillance: Workshop Summary. National Academies Press.

[55] Raytheon (2010). Enabling information sharing: Balancing need to know with need to share. *Technology Today*, 2010 Issue 1.

[56] Raytheon (2013). Secure information access and transfer for dod and intelligence communities. Raytheon Trusted Computer Solutions, 12950 Worldgate Drive, Suite 600, Herndon, VA 20170.

[57] Richter, A.W., Hirst, G., van Knippenberg, D. & Baer, M. (2012). Creative self-efficacy and individual creativity in team contexts: cross-level interactions with team informational resources. *J Appl Psychol.* 2012, 97(*6*):1282-90. doi: 10.1037/a0029359.

[58] Salas, E., Guthrie, J. W., Wilson-Donnelly, K. A., Priest, H. A. and Burke, C. S. (2005) Modeling Team Performance: The Basic Ingredients and Research Needs, in Organizational Simulation (eds W. B. Rouse and K. R. Boff), John Wiley & Sons, Inc., Hoboken, NJ, USA. doi: 10.1002/0471739448.ch7

[59] Saydjari, O.S. (2004). *On the Horizon. Multilevel security: Reprise.* IEEE Security & Privacy. Published by the IEEE Computer Society.

[60] Smith, R.E. (2001). Cost profile of a highly assured, secure operating system. *ACM Transactions on Information and System Security (TISSEC),* Volume 4, Issue 1, 72-101.

[61] Spannuth, K.L. (2002). The most likely nemesis to timely, accurate electronic information. A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the Joint Military Operations (JMO), Naval War College, 686 Cushing Road, Newport, RI 02841-1207.

[62] Sperling, B. K., Pritchett, A., Estrada, A., Adam, G. E. (2006). Information distribution in complex systems to improve team performance. *USAARL Report No. 2006-03.*

[63] Spivey, M.A. (2002). Web-based collaboration technology and requirements for peace operations. Master's Thesis. Naval Postgraduate School, Monterey, CA 93943-5000.

[64] Thomas, J. T., Steele, R. (2012) The Donor-Grantee Trap: How ineffective collaboration undermines philanthropic results for society, and what can be done about it. ISBN-10: 1468177087, ISBN-13: 978-1468177084.

[65] Treece, D. (1999). Moving sensitive U.S. electrons around a coalition environment without spilling any. *IA Newsletter*, Vol. 2, *No. 4*, 3-5.

[66] United States Department of Justice. (2007) Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era. Library of Congress Congressional Research Service Washington, DC.

[67] Weil, S. A., Carley, K. M., Diesner, J., Freeman, J., & Cooke, N. J. (2006). Measuring

[68] Situational Awareness through Analysis of Communications: A Preliminary Exercise. Command and Control Research and Technology Symposium, San Diego, CA.

[69] Winjum, E., Berg, T.J. (2008). Multilevel security for IP routing. In: *Military Communications Conference 2008*, pp. 1–8. IEEE Press, New York.

[70] Zhang, L., Brodsky, A., Swarup, V., & Jajodia, S. (2008). A Framework for Maximizing Utility of Sanitized Documents Based on Meta-labeling. 2008 IEEE Workshop on Policies for Distributed Systems and Networks, IEEE Computer Society, 181-188.

LIST OF ABBREVIATIONS, ACRONYMS, & SYMBOLS

3D	. . .	Three dimensional
711 HPW	. . .	711th Human Performance Wing
AFB	. . .	Air Force Base
AFRL	. . .	Air Force Research Laboratory
ANX	. . .	AFRL-NRO Experiment
C3	. . .	Command, control, and communications
CBIS	. . .	Content-Based Information Security
COP	. . .	Common Operating Picture
CTA	. . .	Cognitive Task Analysis
DoD	. . .	Department of Defense
DTIC	. . .	Defense Technical Information Center
IEEE	. . .	Institute of Electrical and Electronics Engineers
KWKW	. . .	knowledge of who knows what
MLS	. . .	Multilevel security
NASA	. . .	National Aeronautics and Space Agency
NRO	. . .	National Reconnaissance Office
NSA	. . .	National Security Agency
R&D	. . .	Research and Development
RH	. . .	Human Effectiveness Directorate
STK	. . .	Formerly: Satellite Tool Kit Changed to: Systems Tool Kit
TO	. . .	Task Order
WP	. . .	Wright-Patterson

APPENDIX A. Concept for Displaying Information According to Security Clearance Level

Let's imagine a distributed collaborative network with a limited number of assets and users. The network connects three centers of operation (although the total number could be much larger). Each center in turn is connected to one or more data collection sites. The purpose of this hypothetical network is to provide multiple types of status information about land, air, sea, and space assets, as well as intelligence concerning the assets of other nations. The network may provide different types of information during peacetime than when military operations are being planned and executed. For example, the network's function may quickly change from one of providing only status information to one of command and control on an as-needed basis. The network is expected to respond immediately to issues crucial to maintaining national security, and to disaster relief. Personnel at the sites must collaborate with each other to provide a clearer picture of status of assets and to make sense of various intelligence data on the network.

Information shared among the sites is in one of three digital formats: chat, digitized radio messages, or imagery (still images or FMV). All data are automatically classified as TSSCI, TS, S, or U, using one of the automated classification techniques mentioned in the literature cited in the body of this report. All data packets contain metadata tags that include the place of origin, the security classification, where the data was sent, and who has read the data. The information is shared over a network that is appropriate for the security level of each piece of data. At their workstations, users are able to see data appropriate only to their security level and their need to know.

To use his/her own workstation, every user will have both a biometric login and a password (a CAC may also be required). The biometric login will be automatic and unobtrusive, and will be refreshed at variable intervals. Smart software residing on servers at each center will display information appropriate to each user's security clearance. Every user will be able to see the same basic information on his screen (consistent with his/her role), except that information above his/her security level will not be displayed.

Personnel at some collection sites will have the same display as the users at the centers. But their security clearances may be different, thus allowing them to see only part of the information.

The display will allow several options. One of them, which is aimed mainly for top echelon personnel, would allow the user to see from their own display who has which

information. Alternatively, anyone who is collaborating with anyone else would know exactly what information he/she has access to, as well as their clearance level. (This is a key feature. The users won't actually see *all* information, but they will know who has it.)

A description of a hypothetical example for displaying information within an operations center according to security clearance level was started below. However, this task ended before the example could be completed. A visualization of the display's functionality is needed for communicating the benefits to the reader.

Hypothetical example

1. Each center is organized approximately as follows:
    a. Top tier: Management, director, senior coordinator, or commander echelon. *(All cleared at the TSSCI level.)*
    b. Second tier: Engineers, scientists, or analysts. *(All cleared to TS.)*
    c. Third tier: Technicians and support staff. *(All cleared to S.)*
2. Collection sites:
    a. Each center is connected to multiple "collection" sites responsible for collecting information and providing it to the respective center.
    b. Collection sites may be operated by university, government, military, commercial, or private concerns. They could even be individuals.
    c. Security clearances of the personnel at the collection sites are unknown. Also, security clearance levels may be defined differently depending on the requirements of the country where the site is located.
    d. Centers may have any number of collection sites, regardless of location, engaged at any time.
3. Types of classified information that individuals in the three centers may have access to include:
    a. Information sources (which nation or major institution within the country) *(TSSCI)*
    b. How the data were collected *(TSSCI)*
    c. The exact location (coordinates) and number of assets (both human and systems, and attack or defense) *(TSSCI)*
    d. Tactical and strategic plans *(TSSCI)*
    e. Movement of assets, equipment, personnel *(TS)*
    f. Current state or mode of equipment and systems *(S)*
4. Data available on Situation Display:
    a. Trustworthiness of the information

        i. Seen by
            1. Top tier management
            2. Second tier
            3. Third tier
b. Location and types of equipment
        i. Seen by
            1. Top tier management
c. Location and number of ground forces
        i. Seen by
            1. Top tier management
d. Direction of movement of forces and equipment
        i. Seen by
            1. Top tier management
            2. Second tier
e. Status of individual pieces of equipment
        i. Seen by
            1. Top tier management
            2. Second tier
            3. Third tier

APPENDIX B. A Smart Collaboration Tool for Use with Multilevel Security

Ideas expressed in a few of the articles that were reviewed gave rise to the notion of a "smart" collaboration aid (i.e., "tool") for use in a multilevel security (MLS) environment that would allow the user to ask for specific information that he/she needs to do a task. The information would be "smart" in the sense that it is task or situation specific. Perhaps the tool would provide the user with categories of information to choose from, where each category is relevant to the task, situation, or mission. The tool would then scan for all relevant information of the appropriate clearance level that can be shared with the user.

The tool is seen as being most useful where the user has access to some information, but not enough to complete his/her job, or to complete a mission, because of security issues. In other words, he/she lacks complete situation awareness, even though he/she is able to "piece together bits and pieces of information." But there is not enough information being shared among team members because of multilevel security issues. This tool would search for all relevant information available at the appropriate security level for each user. Perhaps it would have the capability to automatically redact information at higher security levels. In some ways, this tool would function similarly to a "search engine" that would search all relevant information at all security classification levels, but would return to the user only the relevant information that is appropriate for the user's clearance, and would redact information at higher levels, thus making available to the user more information than he/she would normally get if manually searching for information appropriate to their security clearance level.

The concept of employing an adaptive interface as an aid for developing accurate shared mental models and situation awareness among team members is not new. The notion is that adaptive interfaces can provide different types of information depending on the user's needs (e.g., what the user is doing, how hard he/she is working, etc.). A similar concept applied in the MLS environment might offer different levels of classified information depending on the operator's clearance level.

Examples of articles supporting this notion are Hall, McNeese, Yen, & Seif-El-Nasr, 2006; and Fernandez Vazquez, Pastor Acosta, Brown, Reid, & Spirito, 2012. A concept put forth by Hall, et al. (2006) suggests the use of simulations to test hypotheses about the situation and possible outcomes that can't be known with certainty because such data could be classified at too high level for the user to access. Simulations aided by a smart tool could help the user see the range of possible outcomes instead of zeroing in on just one or a few.

Fernandez, et al. (2012) mentioned the concept of using smart automation to select specific pieces of information that can be shared with teammates. This would facilitate the development of shared mental models, and increase trust among team members because subjectivity in sharing would be removed, and individuals might be less reluctant to join the team.

Clearly much additional research and study would be required in order to develop a smart collaboration tool for use in the MLS environment.

APPENDIX C. References Relevant to This Research Project

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
(2011) Statement for the Record before the Senate Homeland Security and Governmental Affairs Committee: 'Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration'. Office of the Director of National Intelligence, Washington, DC 20511.	...it remains vitally important to both share and protect networks, intelligence, and associated information - and the systems and networks that support them. As we continue to increase sharing, we must also increase the protections put in place to heighten confidence that the intelligence and information that is being shared is being properly used and protected. This is a matter of managing risk; and people, policies, processes, and technology all play important and interconnected roles in managing that risk. Appropriate policies must be aligned across many information sharing constituencies to include, federal, military, state, local, tribal, private sector, and international partners. These policies must also be consistent with the law, and appropriately address civil liberties and privacy concerns. Cultural attitudes and behaviors must reflect these priorities, and be shaped through appropriate training and incentives. Work on the next generation information sharing environment must begin now and be collaboratively developed with the IC and other stakeholder agencies. Whether classified information is acquired via a computer system, a classified document, or simply heard in a briefing or meeting, we have had "bad apples" who have misused such information before and, unfortunately, we will see them again. That does not mean we should err on the side of not sharing intelligence or information - the risk caused by not sharing the information we have with those who need it is simply too great. Rather, we must put all proper safeguards in place, continue to be forward leaning to find the threat before disclosures occur, be mindful of the risks, and manage those risks in the light of the importance of our mission. p. 6 Working within the broad Government effort that is underway to address the security of classified information in the context of information sharing, the IC's strategy involves three interlocking elements: • The first is ACCESS: ensuring that the right people can discover and access the networks and information they need to perform their duties, but not to information that they do not need. This is a complex matter that is centered on the principle of determining "Need to Know."	*Good modern concepts for achieving MLS.*	http://www.dtic.mil/docs/citations/ADA539585

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	• The second element is TECHNICAL PROTECTION: technically limiting the ability to misappropriate, manipulate, or transfer data, especially in large quantities, such as by disabling or prohibiting the use of removable media on classified networks, including thumb drives and CDs. • The third area is AUDITING and MONITORING: taking actions to give the IC day-to-day confidence that the information access granted to our personnel is being properly used. This involves monitoring and auditing user activity on classified computer systems to identify anomalous activity, and following up accordingly. Technology can record users' actions and support the investigation and prosecution of those who intentionally misappropriate classified information. To enable strong network authentication and ensure that networks and systems can authoritatively identify who is accessing classified information, the IC *CIO* is implementing user authentication technologies and is working with the IC elements to achieve certificate issuance to eligible IC personnel in the first quarter of fiscal year 2012. Important elements in this approach include authentication techniques and the use of attributes (such as clearance level) to determine identities and support mission-based access to intelligence. Finally, audit and monitoring technologies are necessary to ensure that employees' access to intelligence information is recorded and anomalies are detectable. Implementation of audit and monitoring technologies, by providing a reliable record of users' actions, will support our ability to identify and react to apparently inconsistent activities, while also affording a means of deterring errant user behavior. During fiscal year 2012, the IC *CIO* will leverage an Enterprise Audit Framework to enhance the sharing of audit data across the IC elements. In addition to these critical technologies - identity and access management, data protection and discoverability, and a reliable audit - the IC *CIO* continues to look at ways to leverage additional technologies, such as digital management and data loss prevention, to find the "sweet spot" between sharing and protecting intelligence.		

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
(2012) Interagency and Multinational Information Sharing Architectures and Solutions (IMISAS) Project. JS J-7, Joint Development, Solutions Evaluation Division, 116 Lakeview Parkway, Suffolk, VA 23435	The Interagency and Multinational Information Sharing Architectures and Solutions (IMISAS) experiment project focused on developing proposed solutions with the potential to overcome challenges in unclassified information sharing, coordination and collaboration with non-military mission partners. This Joint Concept Development and Experimentation (JCD&E) Enterprise project explored the current unclassified information sharing environment to include existing policies, processes, procedures, local authorities and available tools at several United States Combatant Commander organizations. The IMISAS experiment utilized a humanitarian assistance/disaster relief scenario, but found that principles of unclassified information sharing are applicable across a range of operations. The project's community of interest included the US Department of Defense and other US Government agencies, multinational and coalition, international organizations and non-governmental organizations. This report is comprehensive of the entire project and is separated into six sections and 18 annexes.	*This is a huge report—988 pages—and was not reviewed in its entirety.*	http://www.dtic.mil/dtic/tr/fulltext/u2/a559088.pdf
Accenture, (2009) Increasing Capability to Both Protect and Share Information: A Complete Security Approach to Achieve High Performance in Defense and Intelligence.	Multilevel Security The concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization.14 According to Vincent Fragomene, an executive with Accenture's Defense group, engineering these kinds of solutions takes a strength of experience and knowledge, coupled with a background on how multilevel security should be applied to the Defense Department's rules on handling classified information. All of Accenture's multilevel security and cross-domain security solutions follow strict developmental procedures by which engineers collaborate with assigned government information assurance and certification and accreditation subject matter experts to develop architectural designs before executing the software engineering stage to complete development. This process proved very successful in every fielded and accredited solution to date. Multilevel security solutions like the Multi-Layer Access Solution were developed by Gestalt and MAXIM Systems before these companies became part of Accenture Accenture software engineers have developed the Accenture Multi- Domain Access Solution that creates a multilevel secure and stable operating environment that is transparent to users. This solution can be customized to track crisis situations through Microsoft Windows or UNIX-based programs that allow the required departmental person visibility based on his or her "need to know." Accenture's Multi-Layer Access Solution provides personnel an innovative and authorized		http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Defense_Security_Approach_for_High_Performance_in_Defense_and_Intelligence.pdf

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	way to selectively share sensitive or classified data, both in warfare and in business. This solution is an accredited and certified network-based tool that allows software applications to function in a multilevel secure environment and also enables data providers to support multilevel security customers without needing to be multilevel security aware.		
Ackerman, R.K. (2007) Terrorism, Technology Drive Pacific Intelligence Needs. *Signal;* Oct 2007; 62, 2; ProQuest Advanced Technologies & Aerospace Collection, pg. 23	The prime instrument for exchanging information with Pacific allies is the Combined Enterprise Regional Information Exchange System, or CENTRIXS (*SIGNAL* Magazine, November 2006 and April 2007). The command has the necessary technology to share certain levels and categories of information with nations based on existing relationships, the admiral notes. These links are explored and enhanced through bilateral or multinational exercises. One challenge is that the United States has an established classification and information handling system and process, which many Asia-Pacific nations lack. Most countries operate largely at the unclassified level with occasional forays into the sensitive level, the admiral points out. These nations do not have experience with a tiered multilevel security system, and this touches on both technological and cultural incompatibility. The admiral notes that his office strives to make as much intelligence releasable to as many people as possible, particularly at lower classifications. One solution to this challenge is that PACOM is transitioning its former Joint Intelligence Center–Pacific (JICPAC) to a JIOC, which is being headed by Adm. Singer. He explains that it differs from the JICPAC by changing the way intelligence is processed and disseminated. Instead of being a processing center for intelligence that is regenerated as a standard product, the JIOC is tailoring intelligence to theater-based users. This goes beyond merely customizing the product for the user, he elaborates. For example, good intelligence on a terrorist group in an Asian country would encompass how the terrorists operate, where they live, how they think, whether the populace likes or dislikes them—and why—and what their goals are. That information must be up-to-date and available around the clock. The new JIOC, which should reach its starting point in December, builds on recommendations established after the September 11, 2001, terrorist attacks. One of its key changes is to rely on open source information to a greater degree. Pursuing unclassified information more aggressively generates “tremendously good information” that can be shared with more countries, the admiral points out. The Admiral relates that in a recent information exchange with the Philippines, PACOM	Addressing technology issues is a different challenge. Adm. Singer notes that about one year ago, PACOM shifted to using the Intellipedia (see page 45) to improve intelligence collaboration. While the Intellipedia has worked well, the command still needs cross-domain collaborative tools that will enable it to add higher level capabilities such as voice and chat functions. Another key technology need is for tools that help visualize intelligence knowledge. Instead of analysts writing documents or preparing PowerPoint slides that summarize intelligence information, their product would become a multimedia human-friendly “transfer of knowledge,” the admiral offers. The third need focuses on dissemination. Intelligence personnel must be able to	http://www.afcea.org/content/?q=node/1396

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	determined that 80 percent of the intelligence it was sharing could be supported by a variety of open source material. This meant that 80 percent of the information could be shared at the unclassified level. "More and more, we're finding that the world of 'super secrets' is a smaller percentage of the contribution to our knowledge than the vast amount that is readily available in open sources," Adm. Singer declares. This increased emphasis on open source intelligence sharing helps work around the problem of multilevel security, for which a solution is not imminent. While highly sensitive information can be shared with primary U.S. users, PACOM makes every effort to tailor intelligence so that it can be shared at the Secret level over the secret Internet protocol router network, or SIPRNET, the admiral reports. After that, the command strives to provide that information at the unclassified level.	set up their online site to collaborate, learn and add value to information, and it must be available and up-to-date. And, these activities must be achieved in a multimedia format that is user-friendly. This effort is complicated by differences in the analytic world. Systems and formats differ among signals, human, geospatial and other intelligences—the –INTs. Yet their information must be consolidated quickly to generate intelligence knowledge. This approach employing different types of media parallels Web 2.0 activities, and it draws from many of those enabling technologies, the admiral points out.	
Adigun, A.A., Osofisan, A.O., Robert, A.B.C., & Kolawolfe, M.O. (2012). Adaptive Collaboration in a Dynamic Environment for Information Sharing. *Journal of Emerging Trends in Computing and Information Sciences*, Vol. 3, *No. 7*, 1089—1092.	Collaborative systems are used in learning environment to track problem solving methodology. Previously developed collaborative systems were generally concerned with the evolutions and contributions in dynamic environment. However, when evolutions and dynamism are promoted, information sharing among participants is generally compromised, a problem that has not been well addressed. This study has developed adaptive collaborative systems that enabled reuse of information in a dynamic environment that reduced compromise among participants. Access time for adaptive collaboration in a dynamic environment for information sharing was enhanced. A key stakeholder is any party directly influenced by the actions others take to solve a complex problem. Whilst a collaborative outcome is the development of integrative	*Although not necessarily an important paper for this project, it does define "collaborative system" fairly well in the first paragraph, and attempts to define the features of such system.* *The authors make reference to 'shared mental models' without actually*	http://cisjournal.org/journalofcomputing/archive/vol3no7/vol3no7_14.pdf

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	solutions that go beyond an individual vision to a productive resolution that could not be accomplished by any single person or organization, a collaborative system can engage multiple users or agents in a shared activity usually from remote locations	*using the term.*	
Analytical Graphics, Inc. (AGI). (2010) A Case Study: Integrating STK in a Multi-Level Secure Environment.	Challenge: It is often difficult to transfer STK data from a lower-level network to a higher one, and thus to maintain a synchronized common operating picture (COP) for all networks. Solution: Accenture used STK's plug-in capability to integrate the Accenture Multi-Level Access Solution (AMLAS - a Multi-Level Security data access server) with the STK GUI. AMLAS functionality is available directly through STK toolbars and context menus. Data connections are managed through GUI forms within STK and data is converted to STK objects using the STK Object Model application programming interface. Results: The new system allows STK users direct access to data at or below the classification of their network. Changes made at a lower level are instantly available to higher level users. Because the STK AMLAS client uses the STK Object Model, it will facilitate integration with custom applications developed on the STK Engine platform.		http://www.agi.com/downloads/support/productSupport/literature/pdfs/CaseStudies/0910_CaseStudyAccenture.pdf
Andrews, A., Packard, S., Alberts, C., White, T., & Crane, L. (2000). Defense Healthcare Information Assurance Program (DHIAP) Phase I Composite Evaluation Report. USAMRAA, 820 Chandler St., Ft. Detrick, MD 21702-5014	This report provides a composite view of the findings and conclusions of the MTF Information Security Evaluations conducted as part of DHIAP Phase I. Research found that the security of patient information in the military medical system can be compromised and is at risk. Vulnerabilities are inherent at the local MTF level, caused in part by the centralized selection, administration, and maintenance of mandated health information systems. The report provides two perspectives on DHIAP Phase I research findings and recommendations.	*Perhaps the main reason this report is included is one statement on page 29:* "The Team also heard reports of users sharing accounts and passwords to facilitate operational needs."	http://www.dtic.mil/dtic/tr/fulltext/u2/a404490.pdf
Asynchronous vs. Synchronous Published on *Technology Solutions for Teaching and Research* (http://academictech.doit.wisc.edu.	There are two general strategies for communicating in a blended course: Asynchronous and Synchronous. Each has its advantages and disadvantages. Asynchronous communication and activities take place outside of real time. For example, a learner sends you an e-mail message. You later read and respond to the message. There is a time lag between the time the learner sent the message and you replied, even if the lag time is short. Bulletin board messages can be added at any time and read at your and the learners' leisure; you do not read someone else's message as it is being created, and you	*This may apply mainly to chat.*	http://academictech.doit.wisc.edu/blend/facilitate/communicate

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	can take as much time as you need to respond to the post. Asynchronous activities take place whenever learners have the time to complete them. For example, viewing videos linked to the course site, reading a textbook, and writing a paper are all asynchronous activities [5 [1]]. There are some key advantages to asynchronous collaboration tools. For one thing, they enable flexibility. Participants can receive the information when it's most convenient for them. There's less pressure to act on the information or immediately respond in some way. People have time to digest the information and put it in the proper context and perspective. Another advantage is that some forms of asynchronous collaboration, such as email, are ubiquitous. These days, it's hard to find a co-worker, customer, business partner, consultant, or other party who doesn't have an email account. The drawbacks of asynchronous collaboration are that they can lack a sense of immediacy and drama. There's less immediate interaction. Sometimes people have to wait hours, days, and even weeks to get a response to a message or feedback on a shared document. The lack of immediacy means that information can be out of date by the time someone views it. This is especially true in light of the rapid pace of change in today's business environment [6 [1]]. In contrast, synchronous, or real-time, communication takes place like a conversation. If your class uses only writing-based tools to communicate, the only synchronous communication possible is a chat session. Everyone gets online in the same chat room and types questions, comments, and responses in real time. Synchronous activities may include chat sessions, whiteboard drawings, and other group interactive work. If your class involves multimedia tools, synchronous communication might involve audio or video feeds to the computer. Some “online” courses require learners and teachers to get together at least once (or sometimes several times) in person, by conference call, or through closed-circuit television links. One of the advantages of synchronous collaboration is its immediacy. You can send and receive information right away. This more closely resembles a face-to-face or telephone conversation between two or more people, so can present a more natural way of communicating. The sense of immediacy is more like to solicit a timely response from people. Synchronous collaboration, in general, is more interactive than asynchronous. [4 [1]]		

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	The downside of synchronous collaboration is that not everyone uses it. Although instant messaging, chat, and other such tools are becoming more common, they're still not as ubiquitous as technology such as email. Another drawback is that synchronous collaboration is not as flexible as asynchronous. All the parties involved must be ready and willing to collaborate at a given moment-or the session doesn't work as well. Also, not everyone does well with this kind of collaboration, particularly people who like to think over what they want to communicate		
(2013) Automating Security in SharePoint, Titus.	Fully integrated with SharePoint, administrators can set fine-grained policies that use metadata to authorize or deny a user's access privileges to specific information. In addition, TITUS's solutions can help to raise user awareness and accountability when handling the information by applying classification headers, footers and watermarks. These markings also promote accountability by applying the user's name and a time stamp to downloaded and exported materials. With TITUS Document Policy Manager for SharePoint, headers, footers and watermarks are applied to Microsoft Office documents and PDF documents automatically according to the polices established by the administrator. TITUS Metadata Security for SharePoint can set permissions on items and documents (and any derivation of those) automatically based on the content type of each item. For example, when configuring policies in TITUS Metadata Security, you can include conditions like "if ContentType = Expense Report" and have unique permissions assigned only to items of those specific content types.	*Could TITUS (or similar technology) be used to automatically label data according to security level? Could this be extended to all digital data within a collaborative environment? If data could automatically receive a security classification, then this opens doors to allow appropriate data to be sent to individuals with appropriate clearances.*	http://sharepointmetadataandclassification.typepad.com/blog/2013/06/automating-security-in-sharepoint.html
Banks, A.P & Millward, L.J. (2007) Differentiating Knowledge in Teams: The Effect of Shared Declarative and Procedural Knowledge on Team Performance. *Group Dynamics: Theory, Research, and Practice*, Vol. 11, *No. 2*, 95–106	The relative effects of sharing mental models (typically defined as declarative knowledge structures) and sharing procedural knowledge on team process and performance were assessed. Forty-eight students completed a series of missions as two-person teams using a PC-based tank simulation. The results showed some support for earlier findings. Shared and accurate mental models of the task were related to team process, which was in turn related to team performance. In contrast, shared procedural knowledge was negatively related to team performance. Accurate procedural knowledge was positively related to team performance. Results are discussed in terms of the effect of sharing knowledge in teams on performance, and the implications for team training.	*The results of the cited study could have implications for determining the types of "knowledge" that are provided via the display concept where lower security level personnel do not see or have access to the entire 3D visualization.(See body of this document for a discussion of this unique visualization concept.)*	http://psycnet.apa.org/journals/gdn/11/2/95/

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
Bijon, K.Z., Ahmed, T., Sanghu, R., & Krishnan, R. (2012) A Lattice Interpretation of Group-Centric Collaboration with Expedient Insiders. 8th International Conference Conference on Collaborative Computing: Networking, Applications and Worksharing , Collaboratecom 2012, Pittsburgh, PA, United States, October 14-17, 2012, 200—209.	For various reasons organizations need to collaborate with external consultants, e.g. domain specialists, on specific projects. Many security-oriented organizations deploy multi-level systems which enforce one directional information flow in a lattice of security labels. However, traditional lattice constructions are not suitable for accommodating external consultants, since such consultants are not "true insiders" but rather "expedient insiders" who should receive much more limited privileges than employees. An authorization model for group-centric collaboration with expedient insiders (GEI) has been recently proposed, wherein organizations create groups and replicate the organizational lattice with selected content for such collaborations [4]. Motivated by GEI, in this paper, we formulate a novel lattice construction wherein a new collaboration category is introduced for each new collaboration group, in a manner significantly different from the usual process of defining new security categories in a lattice. In particular, a collaboration category brings together only the required objects and users. We develop a formal model for lattices with collaborative compartments (LCC) comprising administrative and operational parts covering the life-cycle of such collaborations. We formally prove the equivalence of LCC and GEI, thereby precisely characterizing the information flow and security properties of GEI which heretofore had only been informally considered. This equivalence shows that GEI can be realized via LBAC with minimal operational disruptions.	*The bolded text in the abstract seems to be the most relevant part of this paper.*	http://www.profsandhu.com/confrnc/miscconf/collaborateconm12-lcc.pdf
Brown, J.D. & Charlebois, D. (2010) Security classification using automated learning (SCALE) *Optimizing statistical natural language processing techniques to assign security labels to unstructured text.* DRDC Ottawa TM 2010-215.	Automating the process of assigning security classifications to unstructured text would facilitate a transition to a data-centric architecture—one that promotes information sharing, in which all data in an organization are electronically labelled. In this document, we report the results of a series of experiments conducted to investigate the effectiveness of using statistical natural language processing and machine learning techniques to automatically assign security classifications to documents. Our classification techniques prove effective at assessing a document's sensitivity, achieving accuracies upwards of 80%.	*Perhaps automated classification can be incorporated into the MLS concepts discussed in the body of the current report..*	http://www.dtic.mil/dtic/tr/fulltext/u2/a551452.pdf
Bryant, S.A. (2007) Geospatial Informational Security Risks and Concerns of the United States Air Force Geobase Program. AFIT/GEM/ENV/07-M1, Department of the Air	Today's military leaders are faced with the challenge of deciding how to make geospatial information collected on military installations and organizations available to authorized communities of interest while simultaneously restricting access to protect operational security. Often, these decisions are made without understanding how the sharing of certain combinations of data may pose a significant risk to protecting critical information, infrastructure or resources. In this research program, the security implications of the US Air Force GeoBase (the US	The problem is that in many cases, the data is so readily available, whether the Air Force has created it or some commercial source creates it. If someone wants coordinates or any good level of accuracy, they	http://www.dtic.mil/dtic/tr/fulltext/u2/a465293.pdf

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
Force, Air University, *Air Force Institute of Technology*, Wright-Patterson Air Force Base, Ohio.	Air Force's applied Geospatial Information System) program will be explored. The rapid expansion of the use of GeoBase to communities outside of the civil engineering field necessitates an examination of the intrinsic and extrinsic security risks of the unconstrained sharing of geospatial information. This research will explore difficulties encountered when attempting to rate the sensitivity of information, discuss new policies and procedures that have been implemented undertaken to protect the information, and propose technical and managerial control measures to facilitate sharing geospatial information sharing while minimizing the associated operational risks. The challenges of managing classified information have been discussed, but we can quickly see how intertwined these challenges are and the need to overcome these hurdles in the quest of sharing information. For example, consider emergency responders and command and control functions, such as the Survival Recovery Center (SRC) or Damage Control Groups (DCG), abilities to coordinate a safe cordon around a hazardous chemical spill without informative maps and critical geospatial information. If information is not shared and available for the people who need it to respond to emergencies or make command decisions, we have failed to secure ourselves by giving the most to the situation we possibly could. There is data that different agencies and countries need to be able to share, but in some situations this is not happening. Once the data is shared, there are very few controls that remain in place. The reality of the business process is that the government just has to trust that others understand the costs to security. *How is geospatial information classified?* Currently, information is categorized into two main levels of classification, based on the individual merits of the information as either *Classified* or *Unclassified*. However, information that is unclassified is routed into one of three subcategories: 1) Sensitive, but Unclassified, 2) Unclassified, For Official Use Only (FOUO), or 3) Unclassified, Public Information (FOIA). "The fact that this guide indicates that some information may be unclassified does not imply that that information is automatically releasable to the public. Unclassified information…intended for public release must be reviewed for sensitivity and processed through appropriate channels for approval in accordance with DoD Instruction 5230.9, *"Clearance of DoD Information for Public Release"*" (Stenbit, 2003).	could go to Space Imaging or other commercial site and find what they are looking for. What makes this palatable are that it is more difficult to find out which facilities are what, such as command posts, munitions storage, supply warehouses, etc. However, this type of information is slowly creeping from the private domain to the more public domain. The interviews expressed there have been incidents where investigators have had to take maps out of peoples' hands that they have made or had unauthorized access to. Examples in a deployed environment have included escorts finding and confiscating detailed maps from third country nationals (TCNs). Whether they have acquired it from the trash, find it on base, or have one that they have diagramed out on their own, pacing off specific details of the installation. It is much easier to point to the hard copy evidence such as maps found in possession of those without a good need to know, but as far as	

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	"However, in certain circumstances, information that would otherwise be marked UNCLASSIFIED may become classified when combined or associated with other UNCLASSFIED information, if the compiled information reveals an additional association or relationship. See DoD Regulation 5200.1-R. Under such circumstances, it is the combination or compilation of information that is classified, not the individual items of information. Users of this SCG must be aware of such a possibility when compiling UNCLASSIFIED information. Likewise, the compilation of classified information must be classified, at a minimum, at the highest classification within the aggregated data, but may become a higher classification if the compiled information reveals an additional association or relationship" (Stenbit, 2003). Wading into the "Sensitive, but Unclassified" waters, one finds themselves over their head in muddy water. Although the GeoBase administrators and data stewards do their best, they cannot do it in isolation. The Air Force is notorious for allowing decisions to be made at the base level for the best interest of unique situations at each installation. However, with decisions on information classification, continuity amongst how information is to be classified is important across commands and across the service. These determinations must be made and are the most difficult aspect of applying the technological controls. Someone has to make the call on who should be allowed to see what.	the electronic versions of maps and the network, it is much more difficult to evaluate the magnitude of security incidents. As these areas of concern are assessed, one has to consider how fears are fueled or calmed by the feeling of security. The blanket of security helps users feel secure enough to release fears or losing control, power, or that something is going to happen to the data. To overcome these fears and feel more secure about decisions about information, education has been the only way to combat this problem. For years, maps and information have been walking off the installations or can be found publicly on the internet without any kind of control mechanisms in place. Although the perfect solution has not been found, it is better than what it was. There are inherent problems in the system and to be concerned to the point of	

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
		wanting to stop the flow of information now is odd. *Note: This is perhaps the best document on information sharing that was reviewed. The paper asked the question, "Why is so much data classified when it's publicly available on the internet?" Then it talks about the reasons why, although most of the reasons don't have much to do with national security. However, the thought that at least some of the information that individuals with lower level clearances might need is actually available from unclassified sources brings up an interesting question: Can an aid or tool be developed to help them find the information they need? This question is addressed in the body of the present report.* *On page 85, Table 11 "Security Constructs" lists Access Controls. Useful table,*	
Calhoun, C. & Monk, D. (2009) Strategy Planning Visualization Tool (SPVT)	The Air Force Research Laboratory's (AFRL) 711th Human Performance Wing Human Effectiveness Directorate (711 HPW/RHCP) created the Human Effectiveness in the Air & Space Operations Center (HE in the AOC) program to address warfighter work challenges	*This documented was reviewed to determine if any display concepts might*	Volume I: http://www.dtic.mil/

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
for the Air Operations Center (AOC), Volume I: SPVT Summary and COA Sketch, & II: Information Operations (IO) Planning Enhancements. AFRL-RH-WP-TR-2010-0043. Air Force Research Laboratory, 711th Human Effectiveness Directorate, Human Performance Wing, Wright-Patterson Air Force Base, OH 45433.	experienced in the AOC Strategy Division (SD). The research goal was to develop a thorough understanding of warfighter information and decision requirements within the SD and to organizations within and beyond the AOC in order to better support warfighter decision making, affordances and interactions. Phase I of HE in the AOC was conducted by ManTech Aegis and involved a decision-focused analysis of AOC SD personnel. The resulting AOC Cognitive Work Requirements product served as a jumpstart for formalizing user information and decision requirements. Phase II of HE in the AOC consisted of parallel efforts. One effort, Strategy Planning Visualization Tool (SPVT), was tasked with bringing decision-centered visualization support to the Strategy Division Strategy Planning Team (SPT), while the parallel effort, Operational Effects Assessment Visualization Tool (OEAVT), was tasked with bringing decision-centered visualization support to the Strategy Division Operational Assessment Team (OAT). OEAVT was performed by Science Applications International Corporation (SAIC) under a separate contract. SPVT extended the information contained in the AOC SD Phase I Cognitive Task Analysis (CTA) by conducting analyses and performing additional interviews with warfighters. The interaction with warfighters was used to ensure the team had a solid understanding of the CTA, to further develop upon knowledge of work in the AOC SD and to refine concepts and prototypes. The effort yielded an extensive body of knowledge for the AOC SD and resulted in two prototypes, transitioning into Air Force programs of record.	*be applicable to the 3D collaborative environment, and to increase understanding of the information requirements in a collaborative environment such as the AOC.*	dtic/tr/fulltext/u2/a524412.pdf Volume II: http://www.dtic.mil/dtic/tr/fulltext/u2/a518311.pdf
Carley, K.M, Reminga, J., Storrick, J., & Columbus, D. (2011) ORA User's Guide 2011. CMU-ISR-11-107. Center for the Computational Analysis of Social and Organization Systems (CASOS) technical report. Carnegie Mellon University, School of Computer Science, Institute for Software Research, Pittsburgh, PA 15213.	ORA is a network analysis tool that detects risks or vulnerabilities of an organization's design structure. The design structure of an organization is the relationship among its personnel, knowledge, resources, and tasks entities. These entities and relationships are represented by the Meta-Matrix. Measures that take as input a Meta-Matrix are used to analyze the structural properties of an organization for potential risk. ORA contains over 100 measures which are categorized by which type of risk they detect. Measures are also organized by input requirements and by output. ORA generates formatted reports viewable on screen or in log files, and reads and writes networks in multiple data formats to be interoperable with existing network analysis packages. In addition, it has tools for graphically visualizing Meta-Matrix data and for optimizing a network's design structure. ORA uses a Java interface for ease of use, and a C++ computational backend. The current version ORA1.2 software is available on the CASOS website: http://www.casos.ece.cmu.edu/projects/ORA/index.html.	*There are some very interesting network visualizations throughout this document. While perhaps not directly relevant to the current topic, they might be of interest for other projects and applications.*	http://www.dtic.mil/dtic/tr/fulltext/u2/a550789.pdf

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
Cianciolo, A.T., LaVoie, N., Foltz, P., & Pierce, L.G. (2009) Augmented Performance Environment for Enhancing Interagency Coordination in Stability, Security, Transition, and Reconstruction (SSTR) Operations	Stability, security, transition, and reconstruction (SSTR) operations are a core U.S. military mission (United States Department of Defense, 2005). The objective of these missions is to help establish order with the aim of attaining a sustainable peace while advancing U.S. interests. To conduct SSTR operations, U.S. military forces work with a host of partners representing non-governmental aid organizations and other U.S. government agencies, as well as international agencies and multinational military forces. These partners may share an overarching goal, but differ significantly in how the goal or goals should be achieved. The purpose of this effort was to investigate the implications of organizational and national culture on SSTR operations and to define requirements for performance support and training. With a focus on the provincial reconstruction team (PRT), we specified cultural identities (beyond nationality) that influence interagency operations, used consensus-building as a metaphor for understanding SSTR planning, and linked cultural differences to SSTR planning tasks and collective skill breakdowns. A prototype, automated system to enhance interagency collective performance in SSTR operations was demonstrated. The system integrated latent semantic analysis with cultural reference materials, readiness assessments, rehearsal opportunities and individual skill development exercises. Follow on work is planned to refine our understanding of interagency collaboration and implement and test an interagency consensus forum.	*Of some interest here is the* Interagency Consensus Forum (*ICF) prototype, described beginning on page 67. However, it's relevance to the current project is indirect at best, although examples of interagency and international collaboration requirements are of general interest.*	http://www.dtic.mil/dtic/tr/fulltext/u2/a499528.pdf
Cloutier, R. et al. (2013) Prototype of a Graphical CONOPS (Concept of Operations) Development Environment for Agile Systems Engineering. Final Technical Report SERC-2013-TR-031-2. Stevens Institute of Technology, Systems Engineering Research Center, Castle Point on the Hudson, Hoboken, NJ 07030	The goal of the research was to continue the investigation of graphical 3D gaming environments in the construction of a shared mental model during concept development. A result of the research is an artifact that is a "proof of concept" prototype, the CONOPS Navigator. The Navigator is intended to provide a 3D virtual guide through the development of a CONOPS, and also to integrate various tools and applications currently in use. This integration is a widely-sought capability, one which will enable current CONOPS developers and users the flexibility to import and export analysis parameters and results to and from various familiar and well-used tools. Legacy systems are a fact of life in operational concerns; this prototype is intended to demonstrate interconnectivity on a limited scale between specific simulation and mathematical modeling software packages, via a main operational environment. This environment was built using a game development environment. The research includes minor updates to our approaches to implementing, managing, and addressing data impedance challenges between applications including Excel, @Risk, and MATLAB, but the research herein focuses mainly on the development of a use-case scenario-building tool, one capable of interfacing with already-existing battle simulation software.	*If a graphical interface can help collaborators understand each others' CONOPS needs, could a similar visualization help people with lower level clearances get the information they need to do to their jobs, or to communicate to those with higher level clearances their need for information? This paper should be viewed with this idea in mind.* *Note there are two similar reports available; one is much more recent.*	http://www.dtic.mil/dtic/tr/fulltext/u2/a582528.pdf http://www.dtic.mil/dtic/tr/fulltext/u2/a583492.pdf

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
Department of Defense Information Sharing Implementation Plan, April 2009. The Office of the Assistant Secretary of Defense for Networks and Information Integration / DoD Chief Information Officer.	EXECUTIVE SUMMARY The 2006 Quadrennial Defense Review report called for the Department of Defense (DoD) to improve "information sharing with other agencies and with international allies and partners" and to "develop an information sharing strategy" that guides "operations with Federal, State, local, and coalition partners." Accordingly, the Office of the DoD Chief Information Officer (CIO) developed and signed the DoD Information Sharing Strategy on May 4, 2007. It established DoD's vision for achieving effective information sharing across the extended enterprise (i.e., all internal and external participants required to ensure mission success). The Strategy highlighted five implementation considerations to improve DoD's ability to share information: culture, policy, governance, economics and resources, and technology and infrastructure. This plan, the DoD Information Sharing Implementation Plan, addresses those considerations through an initial set of near-term tasks intended to move DoD toward implementing information sharing as envisioned in the Strategy. Additionally, this plan provides amplifying guidance on achieving Goal 2, Information as a Strategic Asset, of the DoD Information Management (IM)/Information Technology (IT) Strategic Plan. The DoD Information Sharing Implementation Plan was developed in coordination with the combatant commands, military departments, and defense agencies. A senior leadership group and its action officers, representing a cross-section of DoD, brought these organizations together through interviews and a workshop to collect their information sharing requirements and concerns. The DoD Information Sharing Implementation Plan represents the results of those efforts. It identifies focus areas and tasks with associated offices of primary responsibility to achieve key information sharing improvements, targeting current and future operations and technologies, within a 36-month timeframe. To make tangible and cost-effective improvements, this plan leverages the successes of existing capabilities and ongoing initiatives that are internal and external to DoD. For example, DoD made substantial progress in developing the infrastructure required for information sharing. This foundation included the physical infrastructure, as well as the associated policies, processes, and personnel for meeting the information demands of DoD missions. The implementation of the DoD Net-Centric Data and Net-Centric Services Strategies, through efforts such as the Maritime Domain Awareness Community of Interest and the Joint Functional Component Command for Global Strike and Integration, resulted in a number of successes in which relevant information was made visible, accessible, and understandable to all authorized users. The DoD Information Sharing Implementation Plan recognizes that organizations' cultures	*Interesting doctrinal document, although not directly relevant to this project.*	http://dodcio.defense.gov/Portals/0/Documents/ISE/DoD%20ISIP%20-%20APR%202009_approved.pdf

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	play a significant role in any successful information sharing environment. This plan identifies tasks to drive cultural transformation as needed to better promote the practice of information sharing. Recognizing that cultural shift alone is not sufficient, the DoD Information Sharing Implementation Plan also addresses management, operations, classification and marking processes, identity and access management, technical infrastructure, and federal government-wide information sharing initiatives. DoD recognizes its responsibility to support its own missions and its role in the broader national information sharing landscape. Accordingly, this plan supports the National Strategy for Information Sharing and other federal initiatives that include areas of cooperation with the Director of National Intelligence, activities from the Federal Information Sharing Environment Implementation Plan, and development of the National Command and Coordination Capability in conjunction with the Department of Homeland Security. DoD-wide support in implementing the tasks outlined in this plan will enable the Department to create an environment that encourages the secure sharing of information to better defend our nation and protect its citizens against the threat of ever-changing adversaries at home and abroad. Together, we will achieve an information advantage for our people and mission partners.		
DoD Information Security Program: Marking of Classified Information, Department of Defense Manual Number 5200.01, Volume 2, February 24, 2012 *Incorporating Change* 2, March 19, 2013.	h. Instant Messaging, Chat, and Chat Rooms (1) Instant messages and chat conversations generally consist of brief textual messages but may also include URLs, images, or graphics. Chat discussions captured for retention or printing shall be marked at the top and bottom of each page with the overall classification reflecting all of the information within the discussion and, for classified discussions, portion markings and the classification authority block shall also appear. (2) Chat rooms shall display system-high overall classification markings (i.e., the highest level of classification allowed to be on the system in accordance with the accreditation of the system being used) and shall contain instructions informing users that the information may not be used as a source for derivative classification unless it is portion marked, contains an overall classification marking, and a classification authority block. i. Attached Files. When files are attached to another electronic message or document the overall classification of the message or document shall account for the classification level of the attachment and the message or document shall be marked in accordance with section 15 of this enclosure.	*Of special importance for this project was the section covering chat, instant messaging, and chat rooms.*	http://www.dtic.mil/whs/directives/corres/pdf/520001_vol2.pdf
DoD Information Security/Website Alert, 06 AUG 2006.	Where collaboration with non-DoD personnel regarding unclassified official information will benefit the department, official *chat rooms* or collaboration sites shall be established and regulated through the use of positive technical controls such as proxy services and screened subnets in accordance with DOD I 8500.2, *information assurance (IA)	*Chat room policy, among other things. Early chat doctrine.*	http://www.js.pentagon.mil/whs/directiv

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	implementation* and approved by the designated approving authority (DAA). Collaboration can take place among DoD personnel or among DoD personnel and authorized non-DoD personnel (including public members of the scientific community) within security and information dissemination guidelines (e.g., export control restrictions). Non-DoD personnel shall be authorized access to the *chat room* or collaboration site on a by-name basis by the DoD sponsor in accordance with procedures established by the DAA. User authentication shall be required for system access.		es/corres/writing/SecDef_Msg_InfoSec.pdf
DTIC Strategic Plan 2011-2016. Defense Technical Information Center, 8725 John J. Kigman Rd., Suite 0944, Ft. Belvoir, VA 22060-6218	*Document does not contain a summary or abstract. It provides DTIC's vision for:* Providing leadership in STINFO policy; providing a knowledge base and analysis of STI; identifying R&E and S&T repositories and offering DTIC users federated access; becoming a catalyst to collaboration across the DoD R&E enterprise; building strong relationships both within DoD and with other partners; exploiting current and leveraging new technologies; balancing access controls with accessibility; creating efficiencies within DoD and DTIC. Balancing access controls with accessibility Understanding that information is only valuable when it is accessible and timely, we will leverage identity management capabilities in the DoD and federal government to simplify access for properly vetted and authorized users, and provide immediate access to users with either authenticated Common Access Cards or Personal Identity Verification (PIV) cards. It is critical not only to protect and share information, but to encourage collaboration and cross-pollination of research. Information assurance, security engineering, identity management, and other data protection and administrative activities must not prevent identified and authorized users from accessing information. The mechanism to identify a user must be accurate, and the determination of authorization must be immediate for DTIC to achieve our mission. DTIC will work with the Defense Manpower Data Center (DMDC) and other providers to offer the best service for our customers. Access delayed is information denied; information that will not be included in research and decision activities. Access is more than simply recognizing credentials. We will review when and where our customers require our support and align to their information needs. We will explore longer support hours, opportunities to co-locate DTIC staff, placement of information assets on the NIPRNET and SIPRNET, and options for DTIC presence at higher network levels. DTIC will examine what is feasible and cost-efficient in terms of Continuity of Operations (COOP) for its systems.	*The points of interest are on page 10.This only supports the view that information needs to be more accessible, with the burden of who accesses it being placed more heavily on access control technology.*	http://www.dtic.mil/dtic/pdf/aboutus/strategic_plan2011.pdf

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
Duley, A.R., Flynn, J., Abich, J., Drabik, H., Szalma, J., & Hancock, P. (2007) Collaborative Technologies and their Effect on Operator Workload in BMC2 Domains. AFRL-HE-WP-TR-2007-0054. Air Force Research Laboratory Human Effectiveness Directorate Warfighter Interface Division Collaborative Interfaces Branch Wright-Patterson AFB OH 45433	A primary goal of this project is to understand how introduction of collaborative technologies affects performance and workload associated with C2 tasks. Accomplishing this goal requires multidimensional measurement of workload and analysis of the associations and dissociations that occur between workload and task performance (Matthews, 2001; O'Donnell & Eggemeier, 1986). Each methodology (performance, physiological measurement, and subjective response) offers a separate vista through which the interaction of workload and human performance can be viewed and therefore provide a more comprehensive and accurate assessment. We intend to transfer the techniques and developed methodologies derived for the measurement of the response of the individual to a companion method aimed at providing a comprehensive analysis of the operational context.	*This article was included because it discusses many issues concerning chat and instant messaging. Under some conditions, collaboration tools such as chat can add to workload, increase distractions, and reduce SA. However, they are also viewed as essential communications tools in today's military and intelligence operations.*	http://www.dtic.mil/dtic/tr/fulltext/u2/a470708.pdf
Eovito, B.A. (2006) The Impact of Synchronous Text-Based Chat on Military Command and Control, Naval Postgraduate School, 1 University Circle, Monterey, CA 93943	This research assesses the impact of synchronous (real-time), text-based chat on military command and control (C2) processes. Chat use among the services, particularly among joint forces, has evolved in ad hoc fashion to fill gaps in currently fielded C2 systems. This growth by- improvisation inhibits clear definition of the underlying requirements: precisely what C2 deficiencies are being addressed by text-based chat tools? Or, from a bottom-up perspective: what capabilities do text-based chat tools bring to the war fighter? In this study we employ a broad set of use-cases to further refine why operators use chat based on how they apply chat to their specific combat problems. These use cases include ongoing combat operations in ENDURING FREEDOM, counter-insurgency operations in IRAQI FREEDOM, and disaster relief operations with Joint Task Force - Katrina. The focus of this study is on establishing operators' perceived requirements in light of the current capabilities delivered by the existing text-based chat tools. From these "reverse-engineered" requirements we propose future work to establish these communication capabilities in the next-generation C2 systems. With most chat residing on the SIPRNET, confidentiality is less at risk by external disclosure than by disclosure to or lack of disclosure from internal users. Many user ids used in chat are functional, making it difficult to know who is really in the chat room. Some consider that human nature creates risk, with users lying about their identity, sharing accounts, failing to log out, account compromise, and somebody looking	*While this report extols the virtues of chat (and there many!), it also points out some risks. The KWKW display concept (described elsewhere in the present document) would incorporate biometric measures to address these risks.*	http://www.dodccrp.org/events/11th_ICCRTS/html/papers/025.pdf or, http://www.dtic.mil/dtic/tr/fulltext/u2/a463372.pdf

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	over your shoulder or even "sniffing" your conversation (JCS and DISA 2005). Malicious software may be received and activated by users if coming from a "person" they are comfortable with in chat (JCS and DISA, 2005). (p 18)		
Eovito, B.A. (2006) An assessment of joint chat requirements from current usage patterns. Thesis, Naval Postgraduate School, Monterey, California.	This research assesses the impact of synchronous (real-time), text-based chat on military command and control (C2) processes. Chat use among the services, particularly among joint forces, has evolved in ad hoc fashion to fill gaps in currently fielded C2 systems. This growth-by-improvisation inhibits clear definition of the underlying requirements: precisely what C2 deficiencies are being addressed by text-based chat tools? Or, from a bottom-up perspective: what capabilities do text-based chat tools bring to the war fighter? In this study we employ a broad set of use-cases to further refine why operators use chat based on how they apply chat to their specific combat problems. These use cases include ongoing combat operations in ENDURING FREEDOM, counter-insurgency operations in IRAQI FREEDOM, and disaster relief operations with Joint Task Force - Katrina. The focus of this study is on establishing operators' perceived requirements in light of the current capabilities delivered by the existing text-based chat tools. From these "reverse-engineered" requirements we propose future work to establish these communication capabilities in the next-generation C2 systems. 1. J-3 Operations *a. Multinational Operations* Her Majesty's Canadian Ship (HMCS) TORONTO (FFH-333) participated in OPERATION ALTAIR (Canadian OEF parallel) in 2004. She deployed as a fully integrated escort of the USS GEORGE WASHINGTON'S (CVN-73) Carrier Strike Group (CSG) to the Arabian Gulf. The CSG exercised C2 with chat over SIPRNET (Secure Internet Protocol Routed Network), which HMCS TORONTO (the CSG's only foreign ship) could not access. Canadian Forces task by voice; however, the CSG used the coalition wide area network (COWAN) chat for tasking HMCS TORONTO, with voice circuits as backup. United Kingdom and New Zealand vessels in the area of operations (AO) were also on COWAN chat. TORONTO stood picket duty in sector screen for the CSG, tasked and coordinated over COWAN chat. Tasking orders for urgent maritime interdiction operations (MIO) were sent to HMCS TORONTO over the COWAN chat and she boarded 123 ships for the CSG. The Combat Officer, HMCS TORONTO summed up chat issues from the Canadian point of	*The relevance of the Navy's chat requirements and the case study are yet to be determined.*	http://www.dtic.mil/dtic/tr/fulltext/u2/a451327.pdf

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	view. The U.S. Navy did not rely on a single chat tool for C2. With HMCS TORONTO as the only non-U.S. warship it was easy for the CSG to overlook the need to use COWAN chat. Even with a liaison officer (LNO) aboard the George Washington and six months together, the U.S. never made the leap to using COWAN and continued using primarily SIPRNET chat. The recommendation was that coalition forces should use coalition networks.		
Espinosa, J.A. & Clark, M.A. (2013) Team Knowledge Representation: A Network Perspective. *Human Factors: The Journal of the Human Factors and Ergonomics Society,* published online 27 June 2013.	KEY POINTS Our research takes advantage of the powerful analytical insights that can be gained from network analysis theories, methods, and tools. ••Our research also builds on strengths of current measures. ••Our research provides computationally simple methods to study team knowledge in the sense that no specialized statistical or network analysis software is necessary and any of the current and popular network analysis tools can be employed. ••Our methods can be applied to study team knowledge at the highest aggregate level, or at any sub-level of detail (members, dyads, slices or cliques), and across multiple team knowledge dimensions of interest. ••Our methods allow us to model individual knowledge attributes that describe content dimensions along with relational attributes that describe structure dimensions, thus providing a more complete picture of the team's knowledge. ••Our methods provide for the computation and visual representation of various dimensions of team knowledge, helping better understand how this knowledge is distributed in the team, thus providing richer and more nuanced explanations of how the distribution of knowledge within a team influences performance and its antecedents.	*Discussion of distribution of knowledge within a team and across teams is relevant.*	http://hfs.sagepub.com/content/early/2013/06/26/001872081349409 3
Fan, X., McNeese, M., & Yen, J. (2010) NDM-Based Cognitive Agents for Supporting Decision-Making Teams. *Human-Computer Interaction*, Vol. 25, pp 195-234.	Naturalistic decision making (NDM) focuses on how people actually make decisions in realistic settings that typically involve ill-structured problems. Taking an experimental approach, we investigate the impacts of using an NDM-based software agent (R-CAST) on the performance of human decision-making teams in a simulated C3I (Communications, Command, Control and Intelligence) environment. We examined four types of decision-making teams with mixed human and agent members playing the roles of intelligence collection and command selection. The experiment also involved two within-group control variables: task complexity and context switching frequency. The result indicates that the use of an R-CAST agent in intelligence collection allows its team member to consider the latest situational information in decision making but might increase the team member's cognitive load. It also indicates that a human member playing the role of command selection should not rely too much on the agent serving as his or her decision aid. Together, it is suggested that the roles of both humans and cognitive agents are critical for	*This article was indirectly responsible for the notion put forth elsewhere in the present document to consider the use of intelligent agents by personnel with the lower level clearances to support decision-making.* *(Only the abstract was available for review.)*	http://www.tandfonline.com/doi/abs/10.1080/07370020903586720

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	achieving the best possible performance of C3I decision-making teams: Whereas agents are superior in computation-intensive activities such as information seeking and filtering, humans are superior in projecting and reasoning about dynamic situations and more adaptable to teammates' cognitive capacities. This study has demonstrated that cognitive agents empowered with NDM models can serve as the teammates and decision aids of human decision makers. Advanced decision support systems built upon such team-aware agents could help achieve reduced cognitive load and effective human-agent collaboration.		
Garfinkel, S.L., Parker-Wood, Huynh, D., & Migletz, J. (2010) An Automated Solution to the Multiuser Carved Data Ascription Problem. IEEE Transactions on Information Forensics and Security, Vol. 5, No. 4, December 2010, 868—882.	This paper presents a novel solution to the problem of determining the ownership of carved information found on disk drives and other storage media that have been used by more than one person. When a computer is subject to forensic examination, information may be found that cannot be readily ascribed to a specific user. Such information is typically not located in a specific file or directory, but is found through file carving, which recovers data from unallocated disk sectors. Because the data is carved, it does not have associated file system metadata, and its owner cannot be readily ascertained. The technique presented in this paper starts by automatically recovering both file system metadata as well as extended metadata embedded in files (for instance, embedded timestamps)directly from a disk image. This metadata is then used to find exemplars and to create a machine learning classifier that can be used to ascertain the likely owner of the carved data. The resulting classifier is well suited for use in a legal setting since the accuracy can be easily verified using cross-validation. Our technique also results in a classifier that is easily validated by manual inspection. We report results of the technique applied to both specific hard drive data created in our laboratory and multiuser drives that we acquired on the secondary market. We also present a toolset that automatically creates the classifier and performs validation.	*Information presented in this article is likely not to be highly relevant to the current effort. However, given the novelty of some of the concepts in the present report, it is difficult to judge the article as not relevant.*	http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA549361
Gavin, N. (2009) STK in a Multi-Level Security Environment. AGI 2010 User's Conference Tour. Accenture.	Accenture has created a client that maintains a synchronized COP for STK users across different networks and security levels. Warfighters and decision makers need the same picture of the battlefield at their fingertips to make informed decisions. But different military personnel have different security classifications, and accessing the same information can be a challenge. During AGI's recent Users' Conference Tour, our good friend Nick Gavin from Accenture shared how his company is resolving this issue for STK users. Getting STK data from a lower-level security network to a higher one usually requires copying the data to a CD and "sneaker-netting" it up. This not only isn't efficient; it delays access to a synchronized common operating picture (COP) from hours to days. Accenture has created a plug-in for STK that gives users instant access to data at or below their classification level.	Reach up to higher level data sources to retrieve data at, and below, current request level Reach down to lower level data sources to include results into high level requests Combine multiple data sources at disparate security levels into a single	http://www.agi.com/downloads/events/2010-users-conference-tour-resources/AGIUC10_MLS_STK_Client.ppt

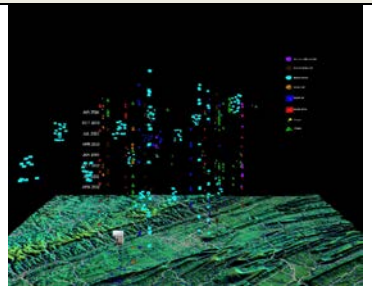
REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	How does it work? The Accenture Multi-Level Access Solution (AMLAS), a Multi-Level Security (MLS) data server, is integrated right into the STK GUI. Data connections are managed through GUI forms within STK and data is converted to objects using our Object Model application programming interface. Sound like something your organization might benefit from? Read the full case study or download Nick's Users' Conference Tour PowerPoint presentation and video. Real-time and near-real-time data visualization Manage data feeds with different clearance levels Automated data scrubbers to pass data to low-side MLS Analysis in STK Create central MLS database for all analysis data Perform STK analysis at lowest possible clearance level throughout project lifecycle Minimize time required on high-level security assets Minimize personnel clearance requirements Allow applications to access data at multiple classification levels Applications need not be multilevel aware Application developers can focus on intended functionality without having to become experts in cross domain computing Multiple data sources appear as a single multilevel database No data stored within AMLAS itself, data providers retain control Integrate legacy systems to provide cross domain data SOAP wrapper provides web-service wrapper for existing applications Immediate integration into SOA	data set JDBC Recordset and/or IC ISM compliant XML return types Programs TENCAP Radiant Alloy CEST/CREST/AMLST Strong Angel Seamless integration with STK All functions accessible from STK Plug-in GUI AMLAS client Format AMLAS data requests Save data to database XML Import and Export IC-ISM compliant XML for classification and control Geography Markup Language (GML) specification Sensor Markup Language (SensorML) specification	or, http://blogs.agi.com/agi/2010/09/23/maintaining-a-synchronized-common-operating-picture-between-networks-of-varying-security-levels/

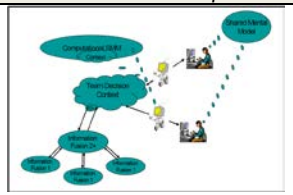
REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	Plug-in based architecture can use legacy applications as data sources to provide standard SQL and/or Web Services access Cross domain certification can be limited to AMLAS and plug-ins Legacy single level systems can continue to operate on isolated single level networks Drastically simplifies certification and accreditation	Conversion to STK Objects Lightweight object capability for visualization of a large number of objects at one time Heavyweight objects for analysis	
Gehres, P., Louthan, G., Singleton, N., & Hale, J. (2010) Toward Sensitive Information Redaction in a Collaborative, Multilevel Security Environment. Conference: International Symposium on Wikis - WIKIS, pp. 1-4, 2010	Wikis have proven to be an invaluable tool for collaboration. The most prominent is, of course, Wikipedia. Its open nature is not suitable for all environments; in corporate, government, and research environments it is often necessary to control access to some or all of the information due to confidentially, privacy, or security concerns. This paper proposes a method by which information classified at multiple sensitivity levels can be securely stored and made accessible via the wiki only to authenticated and authorized users. The model allows for each page to be viewed at appropriate levels of classification transparently included or excluded based on the user's access level. This paper proposes an architecture for a wiki solution that uses a redaction engine to support information sharing under a multilevel security model.	*Could this technology be used to create automatic redaction in an MLS environment?*	http://dl.acm.org/citation.cfm?id=1832793

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
Convertino, G., Wu, A., Zhang, X., Ganoe, C.H., Hoffman, B., and Carroll, J.M. (2008). Designing Group Annotations and Process Visualizations for Role-Based Collaboration. College of Information Sciences and Technology, The Pennsylvania State University, University Park, PA, 16802, 197-206.	Abstract: Team collaboration in situations like emergency management often involves sharing and management of knowledge among distributed domain experts. This study extends our previous research on improving common ground building among collaborators with role-based multiple views, and proposes prototypes of annotation and process visualization tools to further enhance common ground building. We illustrate specific needs through two problem scenarios and propose the designed prototypes through storyboarding. "The costs of not doing enough in a coordinated way far outweigh the costs of doing it... in a coordinated, better way." "We are in a position to do so and we should do it". The EU commission environment spokesperson commenting on the recent forest fire tragedy in Greece, where at least 60 people died. When Greece requested help, nine EU countries responded within 48 hours and all the relief efforts were coordinated through a centre in Belgium (BBC News, Brussels, August 27 2007).	*This group of researchers seems to be doing work related to the goals of this project.* *An idea this article engenders is the notion of a computer database and architecture that can fill in missing information based on probabilities concerning what the missing information could be, in the context of the user's role, and the nature of other available information. When more unclassified information is available, the probability of accuracy would be higher.* *Also, the computer system could determine if any of the classified information is actually available as open source information (perhaps with the source or method of acquiring removed).*	http://zhang.ist.psu.edu/pdf/SBP08.pdf
Grosen. (2013) Nexus Peering: solving the inter-organizational data sharing problem. Palantir website: http://www.palantir.com/2013/07/nexus-peering-solving-the-inter-	How do you implement the right privacy safeguards when sharing data both within and between different organizations? How do you protect data at a granular level, so it can only be accessed by those who are authorized to do so? How do you enable data sharing without compromising data security when different organizations, and different data sources within organizations, are subject to different data protection and retention policies, classification levels, or access control regimes?	"So how does Nexus Peering work? A comprehensive explanation would require more than a simple blog post." *(But the URL link should help.)*	http://www.palantir.com/2013/07/nexus-peering-solving-the-inter-organizati

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
organizational-data-sharing-problem/	Nexus Peering is Palantir's solution to these problems. Nexus Peering enables information-sharing at the institutional level, allowing teams, agencies, and governments to exchange data and analysis in almost any direction or environment while maintaining consistency, integrity, and security.		onal-data-sharing-problem/
Hagen, J.D. (2006). Interagency Collaboration Challenges Among Homeland Security Disciplines In Urban Areas, Naval Post Graduate School, Monterey, CA 93943-5000.	First responders have struggled to incorporate strategic direction provided by the federal government into their existing plans. An urgent call for teamwork and cooperation has changed the landscape for America's first responders. They have been required to shoulder new responsibilities and become more networked and interactive with their peer disciplines to achieve higher levels of performance and response capability. This thesis examines interactions among four key homeland security disciplines in the Seattle, Washington urban area. It evaluates how municipal fire service, law enforcement, emergency management, and public health organizations have used federal government guidance and programs to prepare for catastrophic terrorism response. Specifically, it describes how the homeland security roles, organizational cultures, and collaboration challenges currently facing local public safety agencies have impacted the urban area environment. Based on findings from local and national inquiries, it explains how the National Incident Management System (NIMS) and the National Planning Scenarios (NPS) have impacted interagency collaboration. This study provides a detailed description of the homeland security environment from the inside by identifying challenges facing first responders and the strengths and gaps in their relationships. Finally, it offers positive policy recommendations to Seattle area public safety executives for increasing interagency cooperation in the urban area.	*This article documents interagency collaboration difficulties partially due to MLS issues.*	http://www.dtic.mil/dtic/tr/fulltext/u2/a445405.pdf
Hall, D.L.; McNeese, M.; Yen, J.; & Seif El-Nasr, M. (2006) A Three Pronged Approach for Improved Data Understanding: 3-D Visualization, Use of Gaming Techniques, and Intelligent Advisory Agents. In *Visualising Network Information* (pp. 8-1 – 8-12). Meeting Proceedings, RTO-MP-IST-063, Paper 8.	Applications of multi-sensor fusion span a variety of domains from crisis management, military tactical situation and treat assessment, environmental monitoring, and more recently, monitoring of information systems. Rapid advances in data collection and dissemination provide the opportunity for major improvements in the information gathering aspect. However, a fundamental paradox exists in the understanding side. The paradox is that information analysts are drowning in a sea of data but unable to obtain the knowledge that they need to address difficult problems. This has often been referred to as the data overload dilemma or more recently framed "cogmenutia fragmentosa". On one hand, an unprecedented capability exists to collect data via distributed sensors, commercial information providers, human sources, or Internet resources. Smart micro-scale sensors, wireless communications, and global Internet accessible resources enable the entire earth to be a potential information resource. Such information is available literally at the fingertips of the analysts. However, the wealth of data has not produced a commensurate improvement in analyst abilities. Analysts are literally swamped with data. They have a	*The notion of quickly building game-like scenarios so that lower security level personnel can test hypotheses and ask questions is intriguing. This is not specifically mentioned in the report, but the discussion of The Sims on page 8-8 is interesting. This could be used for visualizing hypotheses. The hypotheses could be shared with those with*	http://www.dtic.mil/dtic/tr/fulltext/u2/a477174.pdf

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
Neuilly-sur-Seine, France: RTO. Available from: http://www.rto.nato.int/abstracts.asp.	wide variety of choices to make as to what is useful and usable, given the context of what they are trying to understand. This paper describes a three-pronged approach to improve information understanding including; (1) use of 3-D visualization and interaction techniques, (2) role-playing gaming (RPG) concepts, and (3) use of team-based intelligent advisory agents (cyber-advisors). The environment promotes rapid development and evaluation of hypotheses regarding evolving complex situations in an environment in which enormous amounts of data and information are available, but for which there is no clear mapping between observables and underlying threat conditions or activities. Use of advanced visualization techniques and gaming concepts assist in focusing the analysts' attention and promotes an interactive, creative analysis process in which hypotheses are formulated, evaluated, criticized, modified, and changed. The use of gaming techniques leverages the skills of new analysts, already experienced in gaming technologies. Comments are made concerning the application of this approach to understanding network information. A new concept of intelligent information interpretation, search and retrieval (I3SR) is being developed by exploring concepts such as multisensory interaction, dynamic computer-guided focus of attention, deliberate synesthesia, utilization of negative space concepts, and adversarial game concepts. This effort uses The Pennsylvania State University Synthetic Environment Applications (SEA) laboratory to explore the use of new multi-sensory interactions: e.g., sound, vision, haptic interfaces. Demonstrations are being developed to explore the concepts identified above and also exploring user/information control and feedback mechanisms. Examples of potential demonstrations include novel, multi-sensor interactions for data display and interaction; utilization of deliberate synesthesia effects, use of negative space and blink comparison concepts, deliberate blurring and transparency of displays and novel *fly by electronic-wire* control concepts.	*higher level clearances. This would allow the high level people to know what the lower level people are thinking—i.e., insight to their mental models. It wouldn't matter if the lower level people had all of the data (since some of it is classified at too high level anyway), but what is important is whether they have the right or an acceptable mental model.* "Once hypotheses are collected through this tool, the game will begin. Analysts can invoke a debate where other analyst teams (composed of virtual and real analysts) try to find contradictions to the hypotheses presented. Analysts would use the tool to drag and drop patterns and maneuver characters, thus showing the contradictions or other possible hypotheses." (p 8-8) The Cyber Advisory Team concept on page 8-8 is also very interesting: "A framework is currently	

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	 Figure 3 shows an example of a situation display in which height above the floor represents time of year, different shapes represent different data types, and sound is used to indicate "goodness of fit" (viz., measure of association) among different data types. We are exploring several directions, based on video gaming, to create tools that would enable analysts to perform their jobs faster and better. Our goal is to explore the utility of video gaming (a) as visualization methods and (b) as interaction models to: 1. Increase productivity of analysts by a) providing an engaging interaction method based on game design patterns and b) providing a visualization method based on game methods. This is based on the belief that next generation analysts are game players and thus are familiar with the visualization methods used in games. Providing a closer visualization method to what analysts are accustomed to will enable them to assimilate information quicker. Game visualization methods have been successfully used in mainstream games to enable quick decision making in a game type environment, where making decisions quickly is an important element of game play. 2. Increase the speed by which analysts extract information by providing an abstract visualization method based on cinematic/theatric techniques that allow users or audience members to grasp the story quickly through the set design, character composition and music. 3. Enhance the quality of hypotheses generated by a) providing a method for visualizing hypotheses to assist in revealing contradictions or visualizing probable hypotheses and b) providing a gaming technique for finding contradictions and holes in hypotheses or stories	being developed to use intelligent software agents to assist in data understanding and situation assessment. The framework is based on a team-based agent environment developed by Yen (Yen et al (2004). In this model, intelligent agents act similar to the way a good human team operates; namely cooperating in a dynamic and positive way, sharing a team mental model of the decision and analysis process, and proactively sharing information among team members to improve their analysis and decision-making performance. The framework developed by Yen includes an architecture, knowledge representation and reasoning methods and internal information exchange language to emulate human teams. In addition, the architecture is based on the recognition primed decision (RPD) model of human teams in complex, dynamic environments.	

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
		 Figure 6: Intelligent Agents as a Virtual Advisory Team The intelligent agent concept will allow creation of a virtual advisory team to support the analysis process (Figure 6). The concept is analogous to a defense or prosecution team that uses a team of special experts, specialists to search for related case studies, analysts to watch jury reactions and others to assist in dynamically preparing and modifying a defense or prosecution. By analogy, analysts are developing an understanding of an evolving situation and creating and assessing hypotheses regarding the case – modifying their approach as more data are uncovered or new interpretations are brought forth. One or more intelligent agents could act as “curmudgeon” agents,	

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
		designed to guard against known cognitive biases such as the confirmation bias (in which a human seeks information that only confirms his or her hypothesis rather than looking for refuting evidence)."	
Harris, C.M. (2002) A Collaborative Visualization Framework Using Jini™ Technology, AFIT/GCS/ENG/02M-04, Department of the Air Force, Air University, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio.	It is difficult to achieve mutual understanding of complex information between individuals that are separated geographically. Two well-known techniques commonly used to deal with this difficultly are collaboration and information visualization. This thesis develops a generic flexible framework that supports both collaboration and information visualization. It introduces the Collaborative Visualization Environment (COVE) framework, which simplifies the development of real-time synchronous multi-user applications by decoupling the elements of collaboration from the application. This allows developers to focus on building applications and leave the difficulties of collaboration (i.e. concurrency controls, user awareness, session management, etc.) to the framework. The framework uses an object sharing approach to share information and views between participants in a collaborative session. This approach takes advantage of several Java technologies (i.e. JavaBeans, Jini, and JavaSpaces). JavaBeans establish a well-known standard for applications to operate within the framework. Jini services provide framework stability and enable code sharing across the network. Objects are shared between remote clients through the JavaSpaces service.	*The relevance of this article is not apparent, but should be evaluated by appropriate SMEs.*	http://www.dtic.mil/dtic/tr/fulltext/u2/a401896.pdf
Hennessy, S.D., Lauer, G.D., Zunic, N., Gerber, B., & Nelson, A.C. (2009) Data-centric security: Integrating data privacy and data security. *IBM J. Res. & Dev*., Vol. 53, No. 2, Paper 2, 2009.	Classifying data according to its permissible use, appropriate handling, and business value is critical for data privacy and security protection. This is essential for compliance with the constantly evolving regulatory landscape concerning protected data. Problems arise when users compromise data privacy and security by overlooking the critical need to manage data according to these requirements. This paper considers the creation and application of data classification systems for security and privacy purposes. It focuses primarily on classifying information in a meaningful way through the use of a partially automated methodology that normalizes and classifies structured data throughout an enterprise. We introduce the three pillars of the data-centric security model, which are based on the data-centric security classification offering by IBM Global Business Services (GBS) and the IBM Research Division. In particular, we describe the data classification pillar of the data-centric security architecture, which provides the framework and method for partially automated classification of data to meet the demands of compliance standards.	*The notion of interest here is that data can be classified automatically and perhaps in real-time. This could mean that the classification process could be flexible enough to permit redaction of information going to lower security clearance personnel in real time. This might allow them to have more information than they normally have*	http://www.research.ibm.com/journal/abstracts/rd/532/hennessy.html

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	Newer approaches for achieving data security require an adaptable control system, one that can be easily modified to satisfy new requirements. One data security model that reflects an increased focus on the importance of data is the data-centric security model (DCSM). This model can be used to bridge the communication gap between the operational business and information technology (IT) departments. The data-centric security (DCS) approach increases interactions between the IT organization and the various business units in order to define data ownership and levels of protection to be applied to classes of information. With business leadership enabled to utilize DCS in controlling and driving security policy, the enterprise is able to address legislative issues surrounding the protection of data privacy. Whether through semantic-aware obfuscation techniques 8 or aligning software requirements with security and privacy policies, 9 DCS provides the core abstractions that enable security.	*access to..*	
Hernandez-Ardieta, J.L., Tapiador, J.E., & Suarez-Tangil, G. (2013) Information Sharing Models for Cooperative Cyber Defence. 2013 5th International Conference on Cyber Conflict K. Podins, J. Stinissen, M. Maybaum (Eds.)	Abstract: The globalisation and increasing complexity of modern cyber security operations have made it virtually impossible for any organisation to properly manage cyber threats and cyber incidents without leveraging various collaboration instruments with different partners and allies. This is especially relevant in certain areas of national security, like the protection of critical infrastructures, where the partnership amongst public and private sectors is paramount to adequately protect those infrastructures from emerging threats. Over the last years consensus has emerged that sharing information about threats, actors, tactics and other cyber security information will play a central role in deploying an effective cooperative cyber defence. Near real-time information sharing has recently gained momentum as a means to redress the imbalance between defenders and attackers. In practical terms, the majority of current efforts in this area revolve around the idea of developing infrastructures and mechanisms that facilitate information sharing, notably through standardization of data formats and exchange protocols. While developing and deploying such an infrastructure is certainly essential to solve the problem of "how" to effectively share information, we believe that some key aspects still remain unaddressed, namely those related to deciding on "what" to share, "with whom", "when", as well as reasoning about the repercussions of sharing sensitive data. In this paper, we argue that effective policies for near real-time information sharing must rely on, at least, two pillars. First, formal models to estimate the subjective value of the information shared should be developed. Second, trust/reputation models that consider the dynamic behaviour and changing factors of the sharing community have to be identified. For the latter, we propose to model information sharing communities as directed graphs, with nodes representing community members and edges modelling sharing relationships	*This seems oriented toward making information more easily shared, deciding the risks, considering the recipients, etc. It gives the impression of operating in near real-time, and making decisions about sharing as the information becomes available or as requests for it occur. Very interesting notions in the context of the current report.*	http://www.researchgate.net/publication/255741958_Information_Sharing_Models_for_Cooperative_Cyber_Defence

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	among them. Relevant properties of both nodes and edges are captured through attributes attached to each of them, which subsequently facilitate reasoning about particular data exchanges. The ability to automatically making sharing decisions requires reasoning over formal structures (models) of most of the relevant elements involved, including the information itself, its value, the risks associated with disclosure (not only by us, but afterwards by partners receiving the information, either inadvertently or on purpose), our perception of the sharing community and the relationships among partners, etc.		
Hinton, G.D. (2006) Multiple Independent Levels of Security: The Changing Face of Range Information Management in the 21st Century. *ITEA Journal* • June/July 2006, pp 11-12.	A variety of MILS solutions have been considered in recent years. The optimum approach to MILS is the implementation of Multilevel Security (MLS), in which a single processing device is designed to segment and route data to the appropriate end user at each node in the network. Chipsets and devices have been developed to facilitate a true MLS network topology, but accreditation of MLS systems has proven elusive, largely due to design costs and the intensive testing required to verify the fidelity of MLS devices. Due to the difficulty of implementing and accrediting MLS, many organizations have adopted a Multiple Security Levels (MSL) approach *(see left side of Figure 1)*. In the MSL approach, security point solutions, such as guards and firewalls, are placed in the system architecture to connect two or more security domains in the "system high" mode of operation. The advantage of this strategy is that "system high" operation is a relatively straightforward security implementation that has been used for many years. As a result, an MSL system can extensively utilize commercial off-the-shelf technology and offers less developmental and accreditation risk. On the downside, the MSL approach may degrade performance and may require the replication of hardware, software, staff and processes in each domain to accomplish the security gateway function at each classification level. Because the "system high" domains may not be entirely independent of each other, one or more guards may be needed to control the flow of any information between the domains. Current MLS systems are custom, single-use designs that utilize very specific security protocols. To make MLS solutions practical for the test and evaluation community, new MLS technologies must be developed. Central to this effort must be a single security processor capable of handling and parsing data from multiple sources at different classification levels. This requires an advanced authentication and verification protocol that ensures information is distributed only to those with appropriate access. It also requires advanced intrusion detection algorithms to prevent unauthorized access or masquerading as an authorized user. Encryption and decryption will be central to all of these processes,	Regardless of the technological approach to MILS that is ultimately used, it is clear that ranges must adapt to this emerging requirement. Coordinated coalition warfare means sharing the right data with the right people at the right level. To test systems and train the forces to operate in this environment, the range community needs to position itself to take advantage of emerging MILS techniques and solutions as they become available.	http://www.dtic.mil/dtic/tr/fulltext/u2/a519791.pdf

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	and the processor must be able to account for multiple encryption schemes that may be employed at all levels of classification. On top of this, all of these functions must be implemented in such a way as to minimize processing delays, ideally in real time.		
Huang, J-B & Yang, M-H. (2009) Estimating Human Pose from Occluded Images. Electrical Engineering and Computer Science University of California at Merced.	We address the problem of recovering 3D human pose from single 2D images, in which the pose estimation problem is formulated as a direct nonlinear regression from image observation to 3D joint positions. One key issue that has not been addressed in the literature is how to estimate 3D pose when humans in the scenes are partially or heavily occluded. When occlusions occur, features extracted from image observations (e.g., silhouettes-based shape features, histogram of oriented gradient, etc.) are seriously corrupted, and consequently the regressor (trained on un-occluded images) is unable to estimate pose states correctly. In this paper, we present a method that is capable of handling occlusions using sparse signal representations, in which each test sample is represented as a compact linear combination of training samples. The sparsest solution can then be efficiently obtained by solving a convex optimization problem with certain norms (such as l1-norm). The corrupted test image can be recovered with a sparse linear combination of un-occluded training images which can then be used for estimating human pose correctly (as if no occlusions exist). We also show that the proposed approach implicitly performs relevant feature selection with un-occluded test images. Experimental results on synthetic and real data sets bear out our theory that with sparse representation 3D human pose can be robustly estimated when humans are partially or heavily occluded in the scenes.	*This may be a similar approach to the others mentioned here.*	http://faculty.ucmerced.edu/mhyang/papers/accv09a.pdf
Hutchins, S. & Bordetsky, A. (2006) NPS Testbed for Team Collaboration Model Validation And Knowledge Tool Application. Office of Naval Research Collaboration and Knowledge Management Workshop, January 24 – 26, 2006. Naval Postgraduate School, Information Sciences Department, Monterey, CA 93943	Dual Goals: 1) Test applicability of using a wireless network for data sharing to facilitate reach back to experts for radiation source analysis and biometric data analysis. 2) Understand and improve the effectiveness of team decision-making in complex, data-rich situations by validating the model of team collaboration. Model of Team Collaboration – Emphasizes cognitive aspects of the collaboration process and includes the major cognitive processes that underlie this type of communication: • (1) individual knowledge building • (2) knowledge interoperability • (3) team shared understanding and • (4) team consensus (Warner, Letsky, & Cowen, 2004). • Validate that these processes exist and how they contribute to team performance through verbal protocol analysis coding of team communications.	*Some of the points made in the paper could be relevant, but would require further consideration.*	http://www.dtic.mil/dtic/tr/fulltext/u2/a514942.pdf

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	• Learn how the EWALL can support collaborative problem solving within the scenarios/ tasks employed in the GIGA CODE Lab.		
Ianni, J.D., Aleva, D.L., & Ellis, S.A. (2012) Overview of human-centric space situational awareness science and technology. Air Force Research Laboratory, Human Effectiveness Directorate, Wright-Patterson AFB, OH 45433	Several organizations within the government and industry are researching ways to help humans understand and react to events in space. Gaining space situational awareness (SSA) is both helped and complicated by the fact that there are numerous information sources that need to be planned (i.e., tasked), collected, processed, analyzed, and disseminated. This paper will outline areas of science and technology (S&T) related to human-centric SSA and space command and control (C2) and discuss related efforts within the Air Force Research Laboratory Human Effectiveness Directorate. A survey of other organizations working SSA human factors will be provided as will suggestions on where more attention may be needed. A large part of the research we are aware of is in support of the Joint Space Operational Center (JSpOC), National Air and Space Intelligence Center (NASIC), and similar organizations. Much recent research has been specifically targeting the JSpOC Mission System which has provided a unifying software architecture and vision.	*Reviewed to grasp concepts of space SA and new display concepts for JSpOC.*	http://www.dtic.mil/dtic/tr/fulltext/u2/a573767.pdf
Ikehara, C.S. & Crosby, M.E. (2010) Physiological Measures Used for Identification of Cognitive States and Continuous Authentication. *CHI 2010*, April 10–15, 2010, Atlanta, Georgia, USA.	This paper describes the work done at the Adaptive Multimodal Laboratory over the past several years regarding physiological measures used for the identification of cognitive states and continuous authentication. These cognitive states include: arousal, fatigue, stress, task difficulty and several more. Continuous authentication is a high security application where the user identification is constantly verified based on physiological sensors. The paper first describes the identification of cognitive states and continuous authentication. Second, is a description of the equipment used to acquire the physiological measures. Finally, several applications using cognitive states and/or continuous authentication are described. Continuous Authentication - Unauthorized access is a major security problem that yearly causes millions of dollars of damage, causes millions of person-hours to correct, causes injuries and in critical cases can cost lives. Authenticating the identity of an authorized user for access to a location or for use of a vehicle or device can be done in three different ways. The first method is by the use of something a person carries, such as a token, key or smart card. The second method is by the use of something a person knows, such as a password or personal identification code. The third method is by the use of a person's unique physical or behavioral attributes.	*Possible technology for proposed collaboration solution.* "Continuous identity authentication can prevent an unauthorized person from slipping in and using the computer system after the initial authentication of the identity of the authorized user." (p. 3)	http://www.eecs.tufts.edu/~agirou01/workshop/papers/Ikehara-CHI2010-BrainBodyBytes2010.pdf

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
Irvine, C.E. & Levin, T.E. (2002) A Cautionary Note Regarding The Data Integrity Capacity of Certain Secure Systems. Department of Computer Science Naval Postgraduate School Monterey, CA 93943	The need to provide standard commercial-grade productivity applications as the general purpose user interface to high-assurance data processing environments is compelling, and has resulted in proposals for several different types of "trusted" systems. We characterize some of these systems as a class of architecture. We discuss the general integrity property that systems can only be trusted to manage modifiable data whose integrity is at or below that of their interface components. One effect of this property is that in terms of integrity these hybrid-security systems are only applicable to processing environments where the integrity of data is consistent with that of low-assurance software. Several examples are provided of hybrid-security systems subject to these limitations. 3.4 Multilevel Security Multilevel systems partition data into equivalence classes that are identified by security labels. Data of different sensitivities is stored in different equivalence classes, such that (the data in) some equivalence classes are "more sensitive than," "more reliable than," or "dominate" [than] (the data in) other equivalence classes. The dominance relation forms a lattice with respect to the labels/classes, assuming the existence of labels for universal greatest lower bound, GLB, and universal least upper bound, LUB. A reference validation mechanism (RVM, see "multilevel management component" in Figures 1, 2 and 3), mediates access to objects, controlling object creation, storage, access and I/O, thereby preventing policy-violating data "leakage" across equivalence classes. For confidentiality policy enforcement, a subject's (e.g., program or component's) ability to write-down or read-up is prevented with respect to the dominance relationship on confidentiality labels; for Biba-model integrity, read-down and write-up are prevented with respect to the dominance relationship on integrity labels. Most multilevel systems today are designed to enforce confidentiality constraints; some of these are also designed to constrain flow between integrity equivalence classes.	*MLS explanation on page 6 is relevant..*	http://www.dtic.mil/dtic/tr/fulltext/u2/a435460.pdf
Jedrysik, P.A., Moore, J. A., Salisbury, C.F., & Holmes, B. (2009) Advanced Visualization and Interactive Displays (AVID). AFRL-RI-RS-TR-2009-115, Air Force Research Laboratory, Information Directorate, Rome Research Site, Rome, New York	The Advanced Visualization and Interactive Displays (AVID) program objectives include the evaluation, exploitation, and development of new concepts in information visualization, display technology, and human-computer interaction (HCI) that provide airmen with a tailored information environment. Building on past in-house programs that researched the technology areas of advanced visualization and interactive displays independently, this program sought to develop integrated technology that would leverage each other's capabilities. The advances made in visualization techniques were developed cognizant of the types of high-resolution interactive display capabilities that were available as well as emerging display technology to be developed under this program. Likewise, the display research benefited significantly from the types of visualizations being developed and steered design decisions in the process. Although visualization and display technology can	*An RI report looking at 2D and 3D display concepts.* *JView II is mentioned.*	http://www.dtic.mil/dtic/tr/fulltext/u2/a499446.pdf

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	be thought of independently, this program developed them as complementary technologies each having an impact on the other's research and development. A state-of-the-art facility has been developed to support advancements in visualization and interactive display technologies. It was designed to serve as a resource for the Air Force Research Laboratory's Information Directorate (AFRL/RI) research that could benefit from the capabilities it provides, allowing other programs to leverage technologies not found in typical research facilities. In so doing also helped guide our research to address the needs of technology users. The work space was thoughtfully designed to serve as a demonstration space for moderately large audiences and as a research space that would foster collaboration amongst scientists. Some of the displays and furniture developed are reconfigurable to accommodate various modes of operation. The majority of the visualization work focused on enhancement of the JView API and developing JView based applications. These applications not only understood the implications of large screen and high resolution displays but were designed with their existence in mind. This meant that visualization components needed to be efficient on memory, but also become more aggressive when resources became available. Applications ranged from visualizing measured antenna data for the Joint Strike Fighter and F-22 to volumetric visualization of the National Airspace System (NAS). The researchers explored concepts ranging from how to display complex airspaces, preserving line attributes over arbitrarily tessellated surfaces, and massive node visualization. Unique high-resolution display systems have been developed that leverage commercial-off-the shelf (COTS) technology whenever possible, augmented by exclusive hardware designed to precisely align multiple projector display configurations. In addition systems have been developed that are extremely portable yet large-scale, and can be set-up in any venue with ease in a timely manner. Future research and development in visualization and interactive displays includes heavy use of non-geographic representations. While the location of an item is important for a subset of decisions, how those items are related will often yield more insight. JView 2 will be developed in order to support graph visualization constructs while also realizing improvements to performance and quality due to the changes to the underlying OpenGL graphics library. While massive geospatial data offers a convenient method for level of detail through its inherent spatialization, non-geographic data does not. This is forcing the JView 2 engine to support graph sizes and constructs that greatly exceed that of standard graphing and display packages. In addition to new content types that are of interest, the		

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	world of computation has radically changed. Multi-core processing is not relegated to a small subset and is now the norm. The JView 2 engine and its components will take advantage of multiple threads in order to utilize the resources as efficiently and effectively as possible. Also planned are extended capabilities for the display alignment systems that were developed under this program, intuitive computer system connectivity to the AVID displays, and integration of touch as an additional mode of input.		
Kim, S-y, Zhu, J., Smari, W.W., & McQuay, W.K. (2006) Security and Access Control for a Human-centric Collaborative Commerce System. International Symposium on Collaborative Technologies and Systems, 2006. (CTS 2006).	The rise of globally distributed computer based workspaces has enabled the incorporation of collaboration in electronic commerce (e-Commerce) systems. Working in collaborative environments with e-Commerce technologies leads to the subject of collaborative commerce (or c-Commerce). C-Commerce creates dynamic collaboration and harnesses organizations' information and knowledge base into a computer-based framework to support personalized access to potentially all participants and information in a given community. One of the main concerns in such a system is security and control of access. Many distributed organizations and individuals want to work together and share their information and knowledge in the process. At the same time, they need to protect their privacy and sensitive information and establish proper protocols for access and sharing activities. This paper discusses a human-centered collaborative commerce system (HCCS) and its security and access control design. Specifically, it presents three security modules and components that will support collaborative exchange and processes. We, then, introduce an improved access control method and algorithm which is role-, group-, and task-based (RGT-based access control) that ensures information and resources access efficiently. Developing further access control algorithms and implementations will be considered in a variety of case studies in future work.	*This article seems is a "must read" for anyone working in areas related to the theme of this report.*	http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1644167&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D1644167 A related article is available here: http://www.wacong.org/wac2006/allpapers/issci/issci_209.pdf

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
Kind, P.A. & Burton, J.K. (2005) Information Sharing and Collaboration Business Plan. Institute, Institute for Defense Analyses (IDA) Document D-3206,.Dept. of Homeland Security, 245 Murray Lane, Bldg. 410, Washington, DC 20233	IDA developed a draft Business Plan that addresses Information Sharing Vision, the "As-Is" status and analysis, the "To-Be" (desire end state) and an implementation plan (road map) including recommended near, mid and long term actions. Key concepts addressed include in depth development of advanced collaboration capabilities, inter-agency and coalition Information Sharing and Collaboration (ISC), detailed capability requirements, and requirements. Also, principal issues in governance, standards and policy, cultural resistance, resources, access and dissemination control, collaboration and architecture. A new Capability Maturity Model for ISC and an extensive ISC glossary are included. The Intelligence Community (IC) has done extensive work maturing and expanding standards and infrastructure to support processing of highly classified data. No such process exists for the equivalent needs in the much larger Sensitive But Unclassified (SBU) and For Official Use Only (FOUO) areas. While the processes for CONFIDENTIAL through TOP SECRET security and transmission are included in the IC structure, the more common needs and applications need to be addressed within the State, Tribal and local governments, some private sector, and even elements of the Federal government and Non-Government Organizations (NGO) whose roles prior to 9/11 were less active from a Homeland Security perspective. Data should flow freely in accordance with agreed business rules. Data need not follow hierarchy, but must follow business rules. Decisions are made hierarchically, but not timely or optimally if data is impeded. Data alone is not sufficient. Knowledge and understanding come from context (metadata) as well as content. Collaboration confirms understanding and enables unified operations. Seamless Environment The mission requirement is to provide an environment that is seamless regardless of seams created by the national security classifications of information or the physical separation of existing networks. Cross-Domain solutions will be used to exchange information between the different security levels in the environment. The Cross-Domain Mechanisms of the environment are designed to facilitate sharing and coordination between different classification levels. A few examples of mechanisms include, *Tearlines* (move information to a lower security domain by extracting the portions that are shareable at that level), *Proxies* (used by a higher level domain user to access Services at a lower level domain while complying with domain security requirements), *Organizational Messaging* (exchange of organizational electronic messages between two	*Of course, what is talked about in this document is pretty high level collaboration—i.e., between agencies. And the document does a very good job of this.* *But also interesting is the more general discussion of information sharing and collaboration especially in the executive summary (starting on p. ES-1).* *"*Knowledge and meaning on an individual basis enable individual action." (p. ES-2*). If this is truly a goal in collaborative systems, then there is a major problem when security clearances prevent sharing of information to lower levels.* "Experts may argue about at which level or at how many levels the sharing should take place, but the objective is to jointly construct shared knowledge, enabling meaning and unified action." (p. ES-2) *Authors provide a* "Data to	http://www.dtic.mil/dtic/tr/fulltext/u2/a446879.pdf

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	domain levels) and *Chat* (synchronous online conversations by multiple users from different domain levels).	Meaning Hierarchy" *on p. ES-1, and a* "From Data Through Collaboration to Coordinated Action*" model on p. ES-2.* *There is an excellent discussion of collaboration from p. 6 through 10. Later, such as on pages 16 through 20, there are specifications for creating an improved collaborative environment.*	
Kiviharju, M. (2012) On multi-level secure structured content. Electronics and Information Technology Division, Finnish Defence Forces Technical Research Centre, Riihimäki, Finland, mikko.kiviharju@mil.fi	*Abstract*—Multi-Level Security, MLS, refers to handling information from different levels of security classification securely by people from different levels of clearance. We propose a structured document format to host data from different classification levels (e.g. RESTRICTED and SECRET) in the same, modifiable document. The document access control is enforced cryptographically - content and access control information is encrypted and digitally signed, but the document structure itself is independent of the adjoining key management architecture. We detail the different security-related metadata and sanitization procedures needed for passing data from a common storage to a user with lower clearance. In this paper we introduced and canonized a structured content format complying to multi-level security practices and the cryptographic access control paradigm. The format was aligned with the XML-standard. We explored the motivation behind different types of elements and their relations, as well as the operation with such a structured document. Our approach was independent of the keying architecture. Future work includes e.g. many open questions from the re-construction of a modified document. On a different track, there is also the task to implement a schema validator and appropriate Filter components for the document.	*This statement from the summary is related to the theme of the current report:* "We detail the different security-related metadata and sanitization procedures needed for passing data from a common storage to a user with lower clearance.	http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6387927&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6387927
Lanahan, J.T. (2011) Need To Share: Flowing Valued Information and Secure Networking. Network Science	*Abstract*—The Flowing Valued Information (FVI) and Need to Share (NTS) project addresses implementation and security issues that arise when multi-national, government and non- government organizations (NGOs), have a mission requirement to readily share information. Current control measures, specifically within the US Department of Defense (DOD), only share information on a "Need to Know" (NTK) basis. This often is restricted to		http://ieeexplore.ieee.org/xpl/articleDetails.jsp?ar

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
Workshop (NSW), 2011 IEEE, 138-143.	a hierarchy of classifications amongst organizations who already have an established trust relationship. This and other primary systems currently in use are often not sufficient enough in a large number of cases militaries and NGOs are finding themselves in today. Present doctrine in military coalition environments allow commanders to declare a "need to share", however, there is no automated method to ensure timeliness and efficiency in distributing information across all entities who have a need for it. These environments also pose an issue of trust in military-NGO scenarios. Similar problems are also found in humanitarian aid and disaster relief (HADR) operations. Even though the information being shared may often be represented the same by all organizations, the infrastructure and protocols for movement and communications rarely are. The FVI-NTS project provides an automated means for supporting organizational information sharing in a trusted manner. It allows organizational authorities to implement automated command policies while maintaining the integrity of the data being shared. FVI-NTS formally proves the coexistence of both NTK and NTS controls. It also provides users an elegant but effective graphical user interface for accessing the above system that can be readily be deployed across many organizations regardless of environment. This front-end functionality expands the domain of possible implementation of FVI-NTS to serve as the standard for future DOD NTS network policies and requirements as well as other organizational groups with similar needs. The software is open source and supports operation on multiple computing platforms simultaneously. It [was] shown that the FVI-NTS project provides solutions to the current problems of trust, security, and flowing valued information when organizations have a need to share in ad-hoc environments. It has also been proven in [5] that this project does not have to replace the existing systems, as it merely extends them allowing for fluid implementation across organizations with well-established security controls and large existing repositories of information classified under legacy access control measures. This paper places the previous results in the context of the potential contribution to military operations and reports on the implementation of an interface which implements the formal security results in a user-friendly manner. Because FVI-NTS only extends existing security models it was thus proven that there indeed is coexistence between NTK and NTS without a loss of confidentiality or integrity. Also provided are thoughts on future work because it is important to note that solving trust relationships and proving the security of information sharing is not enough alone to make the information being shared valuable and that will be the areas that become most vital to a commander in the operational sense whether he is dealing with his own organization or coalition partners. All of these features combined make for a very fast, reliable means of establishing trust in sharing information when time and situation do not		number=6004637

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	allow for the overhead of clearing organizations and processing information with the current methods.		
Lianzhong, L. & Peng, L. (2008). A trusted role-based access control model for dymanic collaboration in a federated environment. International Conference on Industrial Informatics, 2008. INDIN 2008. 6th IEEE	*Abstract*-In the Internet-age, the geographical boundaries that have previously impinged upon inter-organization collaborations have become decreasingly important. However, ensuring secure and authorized access to remote services and information resource in a dynamic collaborative environment is a challenging task. According to some recent literatures, trust between users in different security domains or organizations is an effective method to this problem. However, only trust is not enough because of the complexity and burden of authorization. So we integrate role into our trust model to simplify the management of access control. Moreover, in order to make the dynamic collaboration between different domains more secure, we present the constraint to authorization and operations of the users in foreign domains.		http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4618094
Macklin, T. & Jenket, P. (2005) Achieving Cross-Domain Collaboration in Heterogeneous Environments. RTO-MP-IST-042.	The military community relies on chat and Instant Message (IM) technologies for planning operations and near real-time collaboration. For all of the strengths of chat/IM technologies, they do not lend themselves well to use within conventional cross-domain communications architectures. The United States Naval Research Laboratory (NRL) has developed a portable, hybrid architecture that introduces multilevel security (MLS) technologies into environments comprised of multiple security levels (MSL). This architecture was then used as the framework for integrating various software systems into an enabling capability for cross domain chat. The resultant multilevel chat system utilizes various trusted mechanisms to maintain strong process separation, privilege management, and communications interface control. This multilevel chat system was then used in a limited operational experiment (LOE) to enable users in disparate security domains to collaborate with each other based on a pre-defined, tested, and approved system security policy. Efforts are currently underway to develop a certification profile for this system, as well as for the system's hybrid multilevel architecture. We hope to determine the scalability of this architecture through future operational test scenarios. We are also investigating the scope of the solution set to which this architecture may apply, including multilevel web services. MLS does not enable communication between subjects with differing, non-hierarchical security and integrity policies at all. That is to say, there is no way for a user operating at a security level to chat with a user if that user has a lower security label and a lower integrity label without violating either Bell Lapadula or Biba system policies. Analysis of the properties of the traditional cross-domain architectures indicated that no single one of them was adequate for satisfying the US Navy's requirements for a cross-domain chat system. However, evidence also indicated that it would be possible to develop		http://www.dtic.mil/dtic/tr/fulltext/u2/a469686.pdf

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	a satisfactory solution with a hybrid architecture that exhibited some characteristics of each model. Described is a composite MLS, MSL, and Guarding hybrid security architecture that that can be used to securely enable cross-domain chat. One of the challenges faced by both MLS and UTC-based MSL was ensuring that users could not gain unauthorized access to data by masquerading as another user with a different clearance. …based on favourable performance, security, and operational testing results, the Naval program executive office is planning to transition the ML Chat system into a program of record to support multinational coalition collaboration in heterogeneous operational environments.		
Mercado, A. (2008) Exploring Data Sharing Between Geographically Distributed Mobile and Fixed Nodes Supporting Extended Maritime Interdiction Operations (EMIO). Naval Postgraduate School, Monterey, CA 93943-5000	After the 9/11 catastrophe, insurgents and terrorists have shown us that they will continue to employ asymmetric threats to carry out their objectives, by using any available equipment or any available route to their objective that remains unchecked or unchallenged, like car bombs, suicide bombers, and commercial airplanes. In response, the United States and its allies are focusing harder on data sharing efforts in order to improve the situational awareness (SA) of command and control (C2) structures, to make quicker decisions, and to collaborate with remote experts on chemical, biological, and radiological elements, biometrics, or explosive devices. This thesis discusses the data sharing contributions and features of collaborative tools used onboard a boarding vessel in a riverine area and participating nodes to provide or to enhance the SA and decision making process during EMIOs. As maritime operational experiments, conducted by the Center for Network Innovation and Experimentation (CENETIX), are more successful with each successive MIO experiment, a better understanding for methods of sharing substantial data captured during these operations with participating nodes will be reached. GROOVE V3.0 is a collaborative software supports MLS chat. For further information about this software, read NPS Thesis by Klopson and Burdian, March 2005 or www.groove.net. The Groove collaborative application software saves all the text messaging that goes on between the participants, therefore, participants are able to go back to the Groove workspace and see the entire conversation that took place between them. Furthermore, all files that are saved in the workspace remain there (with a timestamp) until deleted.		http://www.dtic.mil/dtic/tr/fulltext/u2/a483543.pdf

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
O'Malley, S.A. (2009) Free to flow--a paradigm shift for multi-level security data exchange. Air Command And Staff College Air University Maxwell Air Force Base, Alabama.	As information systems evolved within the Department of Defense (DoD), safeguards were developed to protect the information being stored and processed. The levels of protection put in place are commensurate with the potential consequences of inappropriate disclosure, following the US government's policy of information sharing based on need to know. The militarys homeland defense mission and the intelligence and law enforcement communities homeland security mission require greater collaboration. This shift for collaboration necessitates a process for evaluating information exchanges for improved information synchronization between DoD and non-DoD operations. Multi-level security information systems are an approach to solving this challenge. There are a number of technology solutions that facilitate multilevel security information sharing. These solutions involve data replication through trusted interfaces, information passing through controlled protocols, and sophisticated, single systems that allow multiple interfaces at various security levels. Since agencies already have huge investments in their information technology infrastructure, it is necessary to identify solutions that capitalize on existing investments. This research explains the current state of the art in multi-level security technologies, identifies technology gaps, but most importantly, defines an approach to evaluate collaboration solutions against threats to information assurance. The DoD recognizes four distinct operating modes for information systems that contain various classification levels of information: dedicated, system high, partitioned, and multi-level. In a *dedicated* system, all users of the system are authorized access to any of the information that resides on the system. Essentially, the only protection required of the system is access, which can be provided by physical perimeter security. For access to a *system high* system, all of the users are required to have the same clearance level. The user may not have the need to know all the information stored on the system, so mechanisms are in place to prevent information from being disclosed to unauthorized users. Security permissions in today's multiuser operating systems are sufficient for protection. The responsibility of ensuring the permissions are correctly defined lies with the information owner. The *partitioned* system is a special class, as it is similar to system high in that all users have the same clearance level, but at the Top Secret security level, information is also partitioned into special access programs, or *compartmentalized*. Additional protection requirements are required for this operating mode. The *multi-level* system is the unique case, however, because the requirement that all users be cleared to the same clearance level is not enforced. This operating mode has been demonstrated to accrediting authorities that an authorized user can access information cleared for release at his clearance level and below. Likewise, users are unable to access information on the system that is classified at a higher security level.15		http://www.dtic.mil/dtic/tr/fulltext/u2/a538904.pdf

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
Ong, K.L., Nguyen, T., & Irvine, C. (2008) Implementation of a multilevel Wiki for cross-domain collaboration. Conference paper. Naval Postgraduate School, Monterey, CA, USA	The pace of modern warfare requires tools that support intensive, ongoing collaboration between participants. Wiki technology provides a hypertext content-based collaborative authoring and information sharing environment that includes the ability to create links to other web contents, relative stability, ease of use, and logging features for tracking contributions and modifications. Military environments impose a requirement to enforce national policies regarding authorized access to classified information while satisfying the intent of wikis to provide an op en context for content sharing. The Global Information Grid (GIG) vision calls for a highly flexible multilevel environment. The Monterey Security Architecture (MYSEA) Test-bed provides a distributed high assurance multilevel networking environment where authenticated users securely access data and services at different classification levels. The MYSEA approach is to provide users with unmodified commercial-off-the-shelf office productivity tools while enforcing a multilevel security (MLS) policy with high assurance. The extensible Test-bed architecture is designed with strategically placed trusted components that comprise the distributed TCB, while untrusted commercial clients support the user interface. We have extended the collaboration capabilities of MYSEA through the creation of a multilevel wiki. This wiki permits users who access the system at a particular sensitivity level to read and post information to the wiki at that level. Users at higher sensitivity levels may read wiki content at lower security levels and may post information at the higher security level. The underlying MLS policy enforcement mechanisms prevent low users from accessing higher sensitivity information. The multilevel wiki was created by porting a publicly available wiki engine to run on the high assurance system hosting the MYSEA server. A systematic process was used to select a wiki for the MYSEA environment. TWiki was chosen. To simplify identification of errors that might arise in the porting process, a three-stage porting methodology was used. Functional and security tests were performed to ensure that the wiki engine operates properly while being constrained by the underlying policy enforcement mechanisms of the server. An objective in designing the test plans was to ensure adequate test coverage, while avoiding a combinatoric explosion of test cases. Repeatable regression testing procedures were also produced. A conflict between the application-level DA C policy of the wiki and that of the MYSEA server was identified and resolved	*Another example of a tool for permitting a form of collaboration in an MLS environment. The lack of a complete two-way collaboration is somewhat less than ideal for the current project..*	http://www.dtic.mil/dtic/tr/fulltext/u2/a484434.pdf

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
Park, J., Nguyen, D., & Sandhu, R. (2011) On Data Provenance In Group-centric Secure Collaboration. *7th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom*), Orlando, Florida, USA, October 15-18, 2011, 221-231.	Abstract-In this paper, we explore data provenance in a group-centric secure collaboration environment. In collaborations, participating organizations are likely to want certain trustworthiness on the data that are shared from other organizations and some assurance on how the shared data are used by users regardless of their organizations. By utilizing data provenance in group collaboration environment, we can provide the participating organizations with various provenance information that can establish trustworthiness and assurance on the shared data. To achieve this, we first identify what kind of operation information can be and should be captured as provenance data and how this information can be expressed in a formal representation which can be queried via the provenance system for certain utilities. We show the identified provenance data for a group collaboration application can provide some unique provenance utilities such as ability to trace the origins or usages of a shared data object even if it was created in a different organization. We utilize Open Provenance Model (OPM) [13] to capture various group collaboration operations identified in [12] and introduce a provenance system for a group collaboration environment that utilizes Resource Description Framework (RDF) data representations [10] and GLEEN-enabled SPARQL query language [7].	*It seems that knowing where every bit of information is going, where it's been, who originated it, whom has seen it, and its classification level could be useful information, particularly if this information were provided as meta-data in a "label." It could be automatically read and routed appropriately to those with proper security clearances.* *The approach in this paper seems to be for new documents being created from bits and pieces of information from other sources. Provenance is a means for tracking the information.*	http://profsandhu.com/confrnc/misconf/2011collabCom-provenance-camerareadycorrected.pdf
Patel, D.M. & Olson, S. (2012) Information Sharing and Collaboration, Applications To Integrated Biosurveillance *Workshop Summary*. Planning Committee on Information-Sharing Models and Guidelines for Collaboration: Applications to an Integrated One Health	After the September 11, 2001, terrorist attacks and subsequent anthrax mailings, the U.S. government prioritized a biosurveillance strategy aimed at detecting, monitoring, and characterizing national security health threats in human and animal populations, food, water, agriculture, and the environment. However, gaps and challenges in biosurveillance efforts and integration of biosurveillance activities remain. September 8-9, 2011, the IOM held a workshop to explore the information-sharing and collaboration processes needed for the nation's integrated biosurveillance strategy. "At that point it is incumbent upon each department and agency to let their respective officers know what they need to know, and that is often where the breakdown occurs." Also, he observed, public health departments are often left outside the loop. "We are working to alleviate that problem, but we are definitely not there yet." Tan observed that USDA has a specialized part of the organization that is equipped to	*Examples provided of real-world incidents where information sharing was critical to success, but it wasn't always shared. An example is provided on p 37, as well as other places.* *Also, this is one article supporting the view of, "tell us what you need to know" and multiple versions of information may needed for each security clearance*	http://biosurveillance.typepad.com/files/iom-nbic-reports.pdf

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
Biosurveillance Strategy: A Workshop. Board on Health Sciences Policy, Institute of Medicine on the National Academies. The National Academies Press, Washington, DC.	receive classified information, but getting clearances elsewhere in the organization so that information can be disseminated can be a problem. Annelli reiterated that USDA has systems to acquire classified information. The challenge is converting classified information into actionable information that can be more widely distributed for use. "How do we take that information and get it to the people who need to know regardless of their level of security clearance . . . and then down to the state and local level?" Raub added that information can occur in different versions. One version might be promulgated broadly, while another version goes only to people with the appropriate clearance. Annelli pointed out that the person who has information is often the one deciding who else needs to know it, yet that person often does not know what other people need. For example, USDA's Food and Nutrition Service does not buy bean sprouts for the school lunch programs. This piece of information would be useful to add to the messaging, but it may not necessarily be conveyed without special attention to interagency communications. (pp 53-54) Sharing is not automatic, and it is not a technology problem, he said. It is a deeply embedded psychological and social engineering problem. Society encourages anti-sharing strategies, and people are taught to be individualists. Organizations and personnel are appraised by how well they hoard information and are evaluated on the basis of their individual missions, which creates a culture of silos. (p. 37)	*level.* *A very interesting quote supports face-to-face discussions this researcher had with knowledgeable "ops" personnel:* "Furthermore, based on the relationships built over the years, city officials would be confident that they would be told of a threat regardless of their security clearances." *(p. 54, last paragraph)*	
Raytheon/PRNewswire. (2007) Compartmented High Assurance Information Network (CHAIN)	CHAIN is a commercial-off-the-shelf-based security solution that allows for data sharing and collaboration between communities of interest and personnel of varying clearance levels, security caveats, and needs to know. It provides secure services such as e-mail, document control and collaboration, VTC, chat, and white-boarding. CHAIN also provides user-level authentication and role-based authorizations, along with the central management of security policies, which allows the system to quickly change security levels to adjust to the operational situation. Other security features include labeling and control of classified documents and e-mails, content validation, anti-virus protection, and data in-transit/at-rest protection. At CWID 2008, CHAIN successfully provided a secure collaboration environment that exceeded the warfighter's expectations. Warfighters used CHAIN to coordinate missions, review intelligence data, and securely chat about current operations, as well as for mission planning (white-board function). While some warfighters were experienced computer users,		http://www.thefreelibrary.com/Raytheon+Technology+Receives+High+Marks+at+Coalition+Warrior...-a0172518707

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	several were not. Even in those cases, CHAIN's intuitive features (similar to the standard DoD desktop environment) enabled all users to quickly learn and use the IA features		
Raytheon. (2013) Secure Information Access and Transfer for DoD and Intelligence Communities. Raytheon Trusted Computer Solutions.	Secure Information Access Trusted Thin Client® (TTC) allows authorized users to access information on networks of multiple sensitivity levels, from a single desktop, while ensuring compliance with mandated security policy. The TTC Distribution Console server provides network separation on the back end, allowing connectivity to multiple networks from one access point. Features and Benefits Data is not stored locally so it cannot be copied to an external device or transferred Consolidates the user environment; eliminates the need for multiple desktops Integrates with common virtualization and consolidation technologies – Citrix®, Microsoft®, VMware® Single wire to the desktop Support for expandable network connections from the Distribution Console Scalable with failover Remotely managed through a central Remote Access Console (RAC) Substantial savings in cost, space, power, and cooling		http://www.trustedcs.com/resources/brochures/RTCS_DODIC_datasheet.pdf
Relyea, H.G.& Seifert, J.W. (2004) Information Sharing for Homeland Security: A Brief Overview. CRS Report for Congress.	Summary In the aftermath of the terrorist attacks on the World Trade Center and the Pentagon, various recommendations and efforts have been made with the intention of improving information sharing among government entities at all levels within the United States, the private sector, and certain foreign governments, with a view to countering terrorists and strengthening homeland security. The National Commission on Terrorist Attacks Upon the United States (9/11 Commission) is among those to have most recently offered recommendations in this regard in its July 22, 2004, report. The types of information potentially within the scope of such sharing include raw data, which has undergone little or no assessment regarding its accuracy or implications; knowledge, which has been determined to have a high degree of reliability or validity; and intelligence, which has been carefully evaluated concerning its accuracy and significance, and may sometimes be credited in terms of its source. This report reviews some of the principal existing homeland security information sharing arrangements, as well as some projected arrangements in this regard, and discusses related policy, evaluations, and proposed legislation (H.R. 10, H.R. 5024, S. 2774/H.R. 5040, S. 2845/H.R. 5140). It will be updated as events warrant.	*Not sure of the relevance. May be too high level.*	http://digital.library.unt.edu/ark:/67531/metacrs6192/
Richter, A.W., van Knippenberg, D., Hirst, G., & Baer, M. (2012) Creative self-efficacy and	We propose a cross-level perspective on the relation between creative self-efficacy and individual creativity in which team informational resources, comprising both shared "knowledge of who knows what" (KWKW) and functional background diversity, benefit the creativity of individuals more with higher creative self-efficacy. To test our hypotheses, we	*This is the conceptual basis for the KWKW display.*	http://www.ncbi.nlm.nih.gov/pubmed/2

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
individual creativity in team contexts: cross-level interactions with team informational resources. *Journal of Applied Psychology*, 97 (6), 1282-1290.	conducted a multi-level study with 176 employees working in 34 research and development teams of a multinational company in 4 countries. In support of our hypotheses, the link between creative self-efficacy and individual creativity was more positive with greater shared KWKW, and this interactive effect was pronounced for teams of high rather than low functional background diversity. We discuss implications for the study of creative self-efficacy in team contexts.		2800186
Rozenblit, J.W., Barnes, M.J., Momen, F., Quijada, J.A., & Fichtl, T. (2000) Soldier Performance Course of Action (COA) Visualization Aids. ARL-CR-302, University of Arizona Electrical & Computer Engineering Dept., 1230 E. Speedway Blvd., Tucson, AZ 85721, Army Research Laboratory, Aberdeen Proving Ground, MD 21005-5425	The computer revolution has resulted in extending the possibilities of battlespace visualization to the brigade commander and below. However, mobility and bandwidth considerations require that the systems be efficient to reflect the realities of modern combat. The Advanced Battlespace Architecture for Tactical Information Selection (ABATIS) is being developed to be a rapid planning and re-planning experimental environment. ABATIS's object-oriented architecture has the advantage of being able to rapidly construct a three-dimensional battlespace that will accurately represent the essential planning components of a brigade and smaller division battle environment. The basic architecture has been extended to include war-gaming logic as part of the software design, and examples are given that pertain to specific military problems. This capability will allow ABATIS to realize fully the implications of battlespace visualization by creating a human-computer synergy that encourages both human and machine to generate and evaluate possible courses of action and their consequences. The human performance implications are discussed, and particular attention is directed toward research issues related to terrain visualization, automation, decision making, and cognitive biases. Based on the literature, we concluded that distrust of automated and decision support systems was a ubiquitous problem. Interestingly, we also found evidence that complacency and over-reliance on computer solutions stemmed from the same generic problem: lack of understanding of precisely what the computer is doing. These insights prompted a general research strategy to better understand the cognitive dimensions of using visualization as an interface between human and computerized problem solving. If the user understands and interacts with computerized solutions, then he or she can suggest, contradict, and if necessary, override computerized solutions. For this to occur, there has to be a common semantic framework between human and computer (a means of discourse) before any real synergy is possible. ABATIS is a software environment being developed to accomplish this by generating visualization concepts that will create a common semantic framework to forge efficient human-computer collaboration. A number of important human performance issues must be resolved to expedite the	*The usefulness of this document lies in this statement from the Abstract:* "This capability will allow ABATIS to realize fully the implications of battlespace visualization by creating a human-computer synergy that encourages both human and machine to generate and evaluate possible courses of action and their consequences." *The possible relevance to this project is the notion that humans and machines can evaluate possible courses of actions based on incomplete information. If lower security level personnel are responsible for making decisions, and they don't have all the information they need because some of it is classified, then the machine can help evaluate their decisions and offer perhaps better ones, based on*	http://www.dtic.mil/dtic/tr/fulltext/u2/a382305.pdf

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	semantic interface. The two identified as particularly important are effects attributable to the display of probabilistic information and effects attributable to cognitive biases, particularly, the confirmation bias. The working hypothesis is that better visualization methods will lessen the human limitations revealed in the literature. Better understanding of collaborative human-computer problem-solving characteristics will result in a semantic visualization environment that enhances dialogue between these two cognitive entities. The ABATIS environment will be the focus of our effort to understand this dialogue and to develop both principles and visualization concepts that will make future planning and re-planning a faster, easier, and more effective process.	*information that the personnel can't access. These personnel don't have to know that the reason for the machine's suggested course of action is classified, or is based on classified information.* *Also, this paper drives home the difficulties in displaying partial information (due to security) in a 3D environment vs a 2D environment.* *Perhaps it would be necessary to allow some personnel to see only a 2D environment, or a 2D representation of certain objects if a full 3D representation violates security requirements.*	
Rozich, R.T. (2003) A practical method for proactive information exchange within multi-agent teams. Submitted to the Office of Graduate Studies of Texas A&M University in partial fulfillment of the requirements for the degree of Master of Science.	Psychological studies have shown that information exchange is a key component of effective teamwork. In addition to requesting information that they need for their tasks, members of effective teams often proactively forward information that they believe other teammates require to complete their tasks. We refer to this type of communication as *proactive information exchange* and the formalization and implementation of this is the subject of this thesis. The important question that we are trying to answer is: under normative conditions, what types of information needs can agent teammates extract from shared plans and how can they use these information needs to proactively forward information to teammates? In the following, we make two key claims about proactive information exchange: first, agents need to be aware of the information needs of their teammates and that these information needs can be inferred from shared plans; second, agents need to be able to model the beliefs of others in order to deliver this information efficiently. To demonstrate this, we have developed an algorithm named PIEX, which, for		http://repository.tamu.edu/handle/1969.1/1203

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	each agent on a team, reasonably approximates the information-needs of other team members, based on analysis of a shared team plan. This algorithm transforms a team iv plan into an individual plan by inserting communicative tasks in agents' individual plans to deliver information to those agents who need it. We will incorporate a previously developed architecture for multi-agent belief reasoning. In addition to this algorithm for proactive information exchange, we have developed a formal framework to both describe scenarios in which proactive information exchange takes place and to evaluate the quality of the communication events that agents running the PIEX algorithm generate. The contributions of this work are a formal and implemented algorithm for information exchange for maintaining a shared mental model and a framework for evaluating domains in which this type of information exchange is useful.		
Sandip, S., Sekaran, M., & Hale, J. (1994) Learning to coordinate without sharing information. *AAAI-94 Proceedings*, 426-431.	Researchers in the field of Distributed Artificial Intelligence (DAI) have been developing efficient mechanisms to coordinate the activities of multiple autonomous agents. The need for coordination arises because agents have to share resources and expertise required to achieve their goals. Previous work in the area includes using sophisticated information exchange protocols, investigating heuristics for negotiation, and developing formal models of possibilities of conflict and cooperation among agent interests. In order to handle the changing requirements of continuous and dynamic environments, we propose learning as a means to provide additional possibilities for effective coordination. We use reinforcement learning techniques on a block pushing problem to show that agents can learn complimentary policies to follow a desired path without any knowledge about each other. We theoretically analyze and experimentally verify the effects of learning rate on system convergence, and demonstrate benefits of using learned coordination knowledge on similar problems. Reinforcement learning based coordination can be achieved in both cooperative and non-cooperative domains, and in domains with noisy communication channels and other stochastic characteristics that present a formidable challenge to using other coordination schemes.	*Although this is an old article, the concept seems fascinating, if it can be applied to humans. The idea is that personnel with lower level clearances can possibly learn correct responses without access to higher level security information.*	www.aaai.org/Papers/AAAI/1994/AAAI94-065.pdf
Savoie, J. (2004) A strong three-factor authentication device: Trusted DAVE and the new Generic Content-Based Information Security (CBIS) architecture. Defence R&D Canada, Ottawa TECHNICAL	This report has three objectives. The first objective is to provide a description/analysis of the Trusted DAVE activity performed by DRDC Ottawa and its contractors. The second is to describe different systems where the demonstrator produced under this activity could be used. The last is to analyse, study, and compare different types of network/system architectures. The activity involved the development of three elements: A secure design for a three-factor Trusted Device for Authentication and Verification (Trusted DAVE), a device demonstrator implementing some of those design elements, and an authentication and verification demonstration system that utilises the device demonstrator. The purpose of the device is to provide the user interface component to be used as a part of a strong Verification and Authentication (V&A) capability for systems used to process classified or	*User authentication system*	http://www.dtic.mil/dtic/tr/fulltext/u2/a436362.pdf

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
MEMORANDUM, DRDC Ottawa TM 2004-198, November 2004	sensitive data. Four possible systems that could use Trusted DAVE are presented. Two of them are related to the CBIS (Content-Based Information Security) concepts and one integrates CBIS and Kerberos. Finally, three architectures for network systems are presented with their advantages and their limitations. A Generic CBIS architecture covering the one specified in the US CBIS ACTD is defined and compared with the two others. The purpose of the Generic CBIS architecture is threefold: (1) provide an architecture for systems generalizing the US ACTD one, (2) illustrate the architecture's fundamental aspects, and (3) introduce an architecture where Trusted DAVE could be useful. b. is a telephone-sized single physical device with processing power that comprises a fingerprint reader, a token or smart card reader, a keypad or keyboard, and a screen. c. is capable of interacting with a user to collect his/her		
Security Company Statements Anonymous, *Signal;* Feb 2011; 65, 6; ProQuest Advanced Technologies & Aerospace Collection, pg. 74—89. Official publication of the AFCEA.	Many companies' security products are listed and described in this directory. Of special interest is ARGUS SYSTEMS GROUP: www.argus-systems.com. Argus Systems group offers multilevel security (MLS) and cross-domain software for systems ranging from desktops This is a wide range of products including MLS and cross domain software ranging from desktops to enterprise servers using the Solaris operating system. The Pitbull software family includes MLS extensions for te base operating system, along with X Windows, MLS GUI, MLS utilities, MLS networking, trusted/MLS NFS, and a migration path to Solaris 10 for TSOL8 products and architectures. MLS cut-and-paste is supported between Microsoft and other desktop applications, along with per-user upgrade and downgrade authorizations. Pitbull-protected platforms are ideal for cross-domain and coalition architectures and are accredited for use as file servers, mail servers, multidomain dekstops, MLS thin-client servers, and other applications. Pitbull includes additional security functionality such as enhanced login, integrity checking and a kernel-enforced, high-security mode for deployed systems in high-risk environments.		http://www.lib.vt.edu/find/databases/P/proquest-advanced-technologies-aerospace-collection.html
Shen, C., Lin, X., & Shi, Y. (2008) Human pose estimation from corrupted silhouettes using a sub-manifold voting strategy in latent variable space. Pattern Recognition Letters 30 (2009) 421–431.	In this paper, a learning-based framework is proposed for human pose estimation in complicated environments. Human silhouettes extracted from input images are always incomplete and corrupted due to shadows, occlusions, motion blur, or foreground/background color similarity. Given a corrupted body silhouette, our goal is to infer the corresponding pose structure robustly, and to reconstruct the input silhouette as well. The basic assumption of our method is that the body pose (and configuration) can be indicated by some parts (components) of the silhouette given a training data set. Based on this assumption, a robust statistical method is applied to gather the information from uncorrupted components, and to ignore the effects from the outliers. In this method,	*This may be another example of filling in incomplete information based on probabilities.*	http://dl.acm.org/citation.cfm?id=1497668

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	Gaussian Process is used to learn the low-dimensional manifold of visual input data, and to create the sub-manifold corresponding to each component of the silhouette. Different from traditional methods, the likelihood probability is computed by means of a sub-manifold voting strategy based on the learned sub-manifolds. By fusing the likelihood and the prior of human poses, the proposed learning-based framework can specify the location of the input human pose in the latent space. The intrinsic pose and configuration can then be deduced from this location, or be refined after outlier rejection. Experiments show that our approach has a great ability to estimate human poses from corrupted silhouettes with small computational burden. Therefore, it can be applied for tracking initialization, 3D pose estimation, 2D configuration reconstruction in occluded, shadowed and noisy environments.		
Shirmohammad, S. & Georganas, N.D. (2000) Collaborating in 3D Virtual Environments: A Synchronous Architecture, Proc.IEEE 9th Inter. Workshops on Enab. Technol. Infr. For Collabor. Entreprises (WETICE) Knowledge Media Networking workshop	To collaborate in a 3D environment, update messages corresponding to the change in the state of a shared object must be communicated among users. While a lot of research has been done in terms of transmission of update messages representing the motion of avatars and objects, very few works focus on collaboration itself. In this paper, we present an architecture that enables tightly-coupled collaborative tasks to be performed efficiently in virtual environments.	*Some of the concepts in this paper could contribute to an overarching collaborative MLS solution.*	http://www.discover.uottawa.ca/publications/files/shervin-ieee-wet2000.pdf
Son, H. and Kim, C. (2013). "Multiimaging Sensor Data Fusion-Based Enhancement for 3D Workspace Representation for Remote Machine Operation." *J. Constr. Eng. Manage.*, 139(4), 434–444.	In incompletely characterized environments such as construction sites, remote machine operation is the preferred—and sometimes the only—safe and efficient solution for the operation of construction machines. When it comes to the operation of remote-controlled construction machines, a human—machine interface is needed so that even in the case of an unstructured environment (such as a construction site), the operator can interact with the machine in a safe and efficient manner. The human—machine interface needs to have the capability of realistically representing a three-dimensional (3D) workspace that provides information feedback to the remote operator. Workspace representation methods that are currently in use have certain limitations—they are time consuming and labor intensive and require high-performance computers. A major objective of this study is the development of an efficient means of representing a workspace in 3D that has the capacity to provide interactive visual feedback to the operator of remote-controlled construction machines. To achieve this objective, the ability is required to acquire dense, accurate, and visually realistic 3D data that can be converted into high-quality models. This allows creation of a	*This may seem like a "far out" notion, but it gives an idea about how partial information can be used for an effective 3D visualization.*	http://cedb.asce.org/cgi/WWWdisplay.cgi?301252

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	realistic 3D workspace representation of terrain, including objects that might be in proximity to the machine. For this purpose, this study proposes a multi-imaging sensor data fusion-based system employing joint bilateral upsampling, which enhances the quality and availability of the information acquired in such an environment. The field experiment results show that combining data acquired with a complementary multi-imaging sensor setup allows enhancement of the quality of the information available to the remote operator. The resulting task-specific 3D workspace representation can be successfully incorporated into the development of remote-controlled construction machines that require interactive visual feedback. This provides the opportunity to make human—machine interaction more efficient and to improve the remote operation capability by assisting the operator. Moreover, the proposed multi-imaging sensor data fusion-based 3D representation approach has the potential for effective use in a broad class of applications within the construction industry.		
Spannuth, K.L. (2002) The most likely nemesis to timely, accurate electronic information. Naval War College, 686 Cushing Road, Newport, Ri 02841-1207	Fighting enemy cyber attacks--it sounds exciting and many people are ready volunteers to help defeat the external attacks; however, the Department of Defense needs everyone to focus on the relatively mundane, internal (non-enemy) issues. The internal issues are the most likely nemesis to timely, accurate electronic information gathering and management for the Commanders-in-Chief (CINCs). While choosing a hard-to-crack password or developing a Continuity of Operations Plan or testing for interoperability may not sound thrilling, similar actions can spell the difference in getting timely, accurate information to the CINCs. Coming to grips with the numerous internal issues and implementing solutions is not necessarily extremely technical or highly expensive; however, it will require strong advocacy from the CINCs. While DOD ensures background checks are done before someone receives a security clearance for access to classified information, little training is currently required before that same person is allowed to have an account on a network. Training and guidance have not kept pace with the rapid proliferation of networks; therefore, people are doing things that significantly affect network integrity and the information accessible through that network. Also, existing guidance does not always get widely disseminated and/or people are not following it. Enforcement of accountability for actions is non-existent or inconsistent. For example, both training and guidance are critical in password selection--a key prerequisite to network usage. Despite DOD policy dictating minimum standards for passwords, some systems do not require specific criteria; therefore, users often select easy to crack passwords. According to Major General Dave Bryan, USA, Commander of		http://www.dtic.mil/dtic/tr/fulltext/u2/a401116.pdf

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	Joint Task Force-Computer Network Operations (JTF-CNO), the most common password at DOD is "password."1 Additionally, some users have the same password on multiple systems, share passwords with co-workers, do not use password-protected screen savers, or record passwords either on paper in an easily accessible location or in a file on the network. Users want passwords that are easy to remember, the ability to utilize the same password for access to more than one system, and aid co-workers during absences; however, these sloppy practices play right into the hand of a malicious insider. While desiring to trust fellow workers, everyone must "address the sobering fact that a majority of threats to proprietary information today originate within the pool of authorized users."2 As the General Accounting Office's (GAO) chief technologist, Keith Rhodes, said, "workers, disgruntled or not, leave open back doors and work around security measures for convenience."3 If NIPRNET users do not have SIPRNET accounts or do not have a SIPRNET terminal in their work area, there will be a delay until new accounts are created, increased security problems by sharing accounts, or delays due to insufficient number of terminals. however, many actions improving procedures or network enhancements appear individual to one organization and not necessarily applied over all the organizations.15 Rich Pethia, Director of the Computer Emergency Response Team which was established in 1988 to be the point of contact for the Internet community, believes the computer industry focuses its engineering for ease of use and not on ease of security administration. He further states there are not enough technical experts who really know how to set up and manage secure systems properly.20 While CINCs want the easiest, fastest methods to process information, especially during contingencies, a delicate balance between functionality and security needs to be achieved.		
Talmaki, S., Kamat, V.R., & Hubo, C. (2013) Geometric modeling of geospatial data for visualization-assisted excavation. Advanced Engineering Informatics 27 (2013) 283–298	Underground utility lines being struck by mechanize d excavators during construction or maintenance operations is a long standing problem. Besides the disruptions to public services, daily life, and commerce, utility strike accidents lead to injuries, fatalities, and property damages that cause significant financial loss. Utility strikes by excavation occur mainly because of the lack of an effective approach to synergize the geospatial utility locations and the movement of excavation equipment into a real-t ime, three-dimensional (3D) spatial context that is accessible to excavator operators. A critical aspect of enabling such a knowledge-based excavation approach is the geospatial utility data and its geometric modeling. Inaccurate and/or incomplete utility location information could lead to	*Worth reading in detail.*	http://pathfinder.engin.umich.edu/documents/Talmaki%26Kamat%26Cai.AEI.2013.pdf

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	false instilled confidence and be counterproductive to the excavator operator. This paper addresses the computational details in geometric modeling of geospatial utility data for 3D visualization and proximity monitoring to support knowledge-based excavation. The details of the various stages in the life-cycle of underground utility geospatial data are described, and the inherent limitations that preclude the effective use of the data in downstream engineering applications such as excavation guidance are analyzed. Five key requirements - Interactivity, Information Richness, 3-Dimensionality, Accuracy Characterization, and Extensibility – are identified as necessary for the consumption of geospatial utility data in location-sensitive engineering applications. A visualization framework named IDEAL that meets the outlined requirements is developed and presented in this paper to geometrically represent buried utili ty geospatial data and the movement of excavation equipment in a 3D emulate d environment in real-time.		
The Biometric Scan. The Biometric Task Force. Biometric Multiplier: *BTF Works with Local Law Enforcement.*		*The main reason this article is included in the database is as a reminder of the possibility of using facial scan/facial recognition technology as a biometric for positive ID for logging into a secure system. The notion is that a scanner could provide continuous recognition throughout a shift to prevent unauthorized personnel from using a workstation.*	http://www.biometrics.dod.mil/Newsletter/issues/2009/Sep/v5issue3_a1.html *At the time of writing of this report, the web address no longer worked.*

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
Trusted Network Environment (TNE®), *Multilevel Information Access and Sharing.* General Dynamics C4 Systems.	TNE is the leading edge cyber solution in use today by the U.S. Department of Defense and Federal Agencies where multiple coalitions of interest (COI) need a trusted information broker to let them share sensitive information across security boundaries. TNE offers a suite of trusted software applications, utilities, and tools that are fully accredited for cross-domain information sharing. TNE's tools are flexible and scalable enough to allow rapid inclusion of new communities on the fly without compromising the security or integrity of the data. TNE has been in use for 19 years, is certified and accredited at DCID 6/3 PL4 by NSA and DIA and is listed on the Unified Cross Domain Management Office (UCDMO)'s cross domain baseline. TNE offers a range of options to accommodate size, weight, and power (SWaP) requirements and is currently being implemented in network operations center environments as well as on air and sea based platforms. TNE Features at a Glance „„ Multilevel support for many commonly used programs such as Microsoft Office and Adobe Acrobat The ability to cut/copy/paste information between dissimilar sources of information for data fusion capabilities in a fully audited environment „„ Multilevel web and database services to reduce hardware/software costs for external users „„ Multilevel email client with "one window" lookdown at all email „„ Single workstation access to different security domains „„ Multilevel information warehouse in a single database „„ Application security banner indicates classification level on every window launched Extensive secure network protocols: HTTPS, MLS SAMBA/SSH/SSL/NFS „„ Interoperability and integration support available for third party applications such as Google® Earth™ Content filtering and checking, antivirus, integrity checking, audit services, and workflow management		http://www.gdc4s.com/trusted-network-environment-(tne).html?taxonomyCat=131

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
United States Department of Justice. (2007) Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era. Library of Congress Congressional Research Service Washington, DC.	The need to develop and share information and intelligence across all levels of government has significantly changed over the last few years. The long-standing information sharing challenges among law enforcement agencies, public safety agencies, and the private sector are slowly disappearing. Yet, the need to identify, prevent, monitor, and respond to terrorist and criminal activities remains a significant need for the law enforcement, intelligence, public safety, and private sector communities. Through the support, expertise, and knowledge of leaders from all entities involved, the fusion center concept can become a reality. Each official has a stake in the development and exchange of information and intelligence and should act as an ambassador to support and further this initiative. It is the responsibility of leadership to implement and adhere to the *Fusion Center Guidelines*.*[continues from here…]*	*There is much relevant information in this document. However, the primary interest was in the thoughts similar to this quote from page 49:* "Rather than rely on clearances, fusion centers should attempt to declassify information and intelligence, when possible, to disseminate to public safety and private sector partners."	http://www.dtic.mil/dtic/tr/fulltext/u2/a470028.pdf
Weil, S.A., Freeman, J., Carley, K.M., Cooke, N.J., & Diesner, J. (2006) Measuring Situational Awareness through Analysis of Communications: A Preliminary Exercise. Command and Control Research and Technology Symposium (CCRTS) 2006	Network centric warfare promises to increase information sharing and allow distribution of decision making. This will improve military effectiveness, but only if the situational awareness (SA) of warfighters is correctly aligned. Modern natural language processing techniques, such as Network Text Analysis (Carley, 1993), are designed to infer the cognitive states of individuals and groups engaged in cognitive collaboration and measure group SA by exploiting data on the information that team members access and generate. An integrated software application, IMAGES, utilizes AutoMap (Diesner & Carley, 2004) as the primary analysis engine to take advantage of the large amounts of communication and report text that naturally occur in collaborative environments. The text generated in the normal course of work is collected and changed into forms that can be compared and analyzed. A comparison of networks based on text from several individuals or groups yields information about the similarity of their respective mental models. Differences among maps may reflect misalignments of SA, which can be remedied by information sharing and targeted communication. An exercise was conducted to assess the potential of NTA as implemented in AutoMap and IMAGES. The results indicate that NTA will allow analysts to effectively assess SA through passive means. Simply put, individuals working together within an organization are more effective when they have the information that is essential for accomplishing their individual tasks. (p. 5) There have been comparatively few resources expended to assess the impact of this infrastructure on an organization's knowledge, ability to maintain fleeting states of knowledge (i.e., SA), or methods to manipulate it. There are however, some tools that do	*There is another discussion of FORCEnet starting on page 3. FORCEnet seems like a necessary but never ending effort to integrate the Navy's various information technologies (including collaborative) and tools into a functional architecture (see page 4).* *The main reason this article is in the database is because of its discussion of shared mental models.*	http://www.dtic.mil/dtic/tr/fulltext/u2/a463341.pdf

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	just this; e.g., AutoMap (Diesner and Carley, 2004; http://www.casos.cs.cmu.edu/projects/automap/) and ORA (http://www.casos.cs.cmu.edu/projects/ora/) which we are using. (p. 5) at the level of the organization, two types of SA are generally acknowledged. There is information that needs to be shared among all team members or subsets of them. We will call this *shared SA*. There is also information that needs to be held by the team as a whole, but not necessarily by every team member. We will call this *team SA*. (p. 5) Team research has shown that effective team performance and team SA requires team members to hold common mental models or cognitive representations of tasks and the team (Cannon-Bowers, Salas, & Converse, 1993; McComb, 2005; Graham, 2005). These shared mental models allow team members to coordinate, often implicitly, within their team. (p. 6) The *team mental model* contains knowledge regarding the individual's role in the task as well as the role of others. (p. 6) Although the team mental model allows members to form expectations and predict future performance regarding how members are likely to act in a situation, the team interaction model takes it a step further by allowing members to anticipate and sequence their collective actions. Thus the team mental model especially affords team situational awareness. (p. 6) Specifically, it has been argued that not only must members hold accurate mental models, but that it is the sharing of mutual mental models among members – or *shared mental models* – that allows for effective coordinated and adaptive team behavior (see Converse et al., 1991; Orasanu, 1990; Cannon-Bowers & Salas, 1990). (p. 6) In network-centric warfare and similar collaborations there is rich information in the interactions among team members that should not be overlooked.(p. 7)		

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
Winjum, E. & Berg, T.J. (2008) Multilevel security for IP routing. Military Communications Conference, 2008. MILCOM 2008. IEEE	This paper presents a multilevel security (MLS) scheme for routing information. Based on an unprotected IP network, MLS routers may establish logical networks that fulfill different sets of security requirements. We describe a routing scheme for separation of routing information into different security classes derived from multiple levels of integrity, confidentiality and availability. The scheme may be useful in coalition networks where partners may benefit from joint resources and at the same time control the security of routes involving its own routers. On the other hand, from a coalition point of view, partner-specific classifications of links and routes may affect the network connectivity. The paper also analyzes this impact.	*The usefulness of this article for the current project should be determined by appropriate subject matter experts.*	http://www.cse.msstate.edu/~ramkumar/mlip.pdf
Wolter, C & Meinel, C. (2010) An approach to capture authorization requirements in business processes. *Requirements Engineering*, 15, 359-373.	Business process modelling focuses on the modelling of functional behaviour. In this article, we propose an extension for the business process modeling notation to express non-functional authorisations requirements in a process model to enable the collaboration between security experts and business analysts. To capture multi-level, role-based and Separation of Duty authorization requirements, new model element attributes and authorisation artefacts are introduced. To enhance the usability of this approach, simple visual decorators are specified to ease the communication of requirements between various stakeholders. To provide an early validation of these authorisation requirements during the definition of a process model, formal semantics are applied to the process model and model-checking techniques are used to provide feedback. As a pragmatic proof-of-concepts, a first prototype implementation is briefly discussed. The Bell-La Padula model is tranquil, which means subjects get clearances and objects are classified following the given rules above and the access control data do not change. Nevertheless, it has been demonstrated that the No- Write-Down requirement is too restrictive in commercial and military applications [19]. In general, the problems have to do with combining data in different compartments and downgrading it after sanitisation. Multi-level and lattice-based security models offer little help here. Therefore, the concept of trusted subjects or downgraders has been introduced to relax the requirement and to allow the flow of information from high to lower clearance levels for trusted subjects. Therefore, we introduced new properties to capture the most prominent authorisation requirements, such as multilevel access control, role-based access control and Separation of Duty requirements. As suggested in [8], additional standard artefacts have been added to the BPMN specification. Taken together, the new authorisation condition artefact and the authorisation requirement decorators we propose provide early visibility of the complete set of requirements to business stakeholders, business analysts, security experts and system implementers.	*Contains mathematical equations and set theory. This article would need in depth study.*	http://link.springer.com/article/10.1007/s00766-010-0103-y

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
Zhang, L., Brodsky, A., Swarup, V., & Jajodia, S. (2008) A framework for maximizing utility of sanitized documents based on meta-labeling. 2008 IEEE Workshop on Policies for Distributed Systems and Networks. Proceedings of a meeting held 2-4 June 2008, Palisades, New York, 181-188.	Document sanitization, i.e., the process of removing or generalizing sensitive information in order to reduce the security classification of the document, is widely used today in applications of information sharing. Traditional document sanitization systems focus on removal or generalization of certain words and phrases, but do not take into account the utility of the sanitized documents. This leads to a gap between the sanitized documents and the users' requirements. Proposed in this paper is a formal framework and conceptual algorithms for optimal document sanitization based on meta-labeling. Each document is associated with a meta-label, which serves to determine both the security label and the utility of the document. In the sanitization process, the system first computes a new meta-label for the sanitized version and then sanitizes the document through mediators guided by the new meta-label. Algorithms are provided to compute a new meta-label that is proven to satisfy the security requirements and provide maximal utility with respect to users' requirements, which are also represented by a meta-label. The problem of how to sanitize documents in order to satisfy the security requirements, and yet to provide the best possible answer to information consumers is exactly the focus of this paper. One well-studied information sharing policy requirement, loosely stated, is to prevent the flow of sensitive information to the wrong entities; this is typically enforced by mechanisms such as multi-level secure (MLS) systems or multiple independent levels of security (MILS) systems. A second policy requirement that has gained prominence in recent years is to ensure that the right entities can access the right information at the right time; this is typically implemented via cross-domain solutions such as "downgraders" or "security guards". While traditional access control methods address the above requirements, they are inadequate for information sharing on a large scale (e.g., see [10]), because the required classification and clearance processes are too rigid and slow for large volumes of dynamically collected information. We believe [traditional access control methods] have two key deficiencies: (1) they aim to limit the risk of disclosure and do not balance that risk with the benefits of information sharing, and (2) they lack sufficient granularity of information objects and hence objects deemed sensitive typically contain valuable information of lower sensitivity. To address the first deficiency, several researchers have suggested risk-based approaches to information sharing (e.g., [13, 10, 2, 4, 5, 9]. The second deficiency is typically handled via document sanitization mechanisms that remove sensitive information from documents in order to reduce the security classification of the redacted documents. However, existing document sanitization systems [12, 8] focus on removal of certain words and phrases, but do not take into account the utility of the sanitized documents, or the reason for the higher sensitivity of	*Contains mathematical equations and set theory. The article would need in depth study.*	http://dl.acm.org/citation.cfm?id=1444452.1445730

REFERENCE	RELEVANT MATERIAL COPIED FROM REFERENCE	NOTES & QUOTES Italicized *text provided by an author of this report.*	URL
	the information. We view document sanitization as a two-step process. First, a decision is made on how to sanitize. Then, a mediator, which is either a human or automated process, modifies the document according to the decided output requirements.		