REPORT DOCUMENTATION PAGE

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
30 NOV 08	FINAL REPORT	01 DEC 05 TO 30 NOV 08

4. TITLE AND SUBTITLE
INFORMATION OPERATIONS ACROSS INFOSPHERES

5a. CONTRACT NUMBER
FA9550-06-1-0045

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
DR THURAISINGHAM

5d. PROJECT NUMBER
2311

5e. TASK NUMBER
FX

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
UNIVERSITY OF TEXAS AT DALLAS, ISSUES IN SCIENCE TECHNOLOGY
2601 N FLOYD RD
RICHARDSON, TX 75080-1407

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AFOSR/NL
875 NORTH RANDOLPH STREET
SUITE 325, ROOM 3112
ARLINGTON, VA 2203-1768

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE. DISTRIBUTION IS UNLIMITED

13. SUPPLEMENTARY NOTES

20100621223

14. ABSTRACT
This research directly supports the Air Force vision of information dominance and the development of [illegible] information systems like the Joint Battlespace Infosphere for C2 support to the warfighters.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(Include area code)*

AIR FORCE OFFICE OF SCIENTIFIC RESEARCH

DTIC Data

Purchase Request Number:	FQ8671-0700211
BPN:	F1ATA06212B010
Proposal Number:	05-NM-225
Research Title:	INFORMATION OPERATIONS ACROSS INFOSPHERES
Type Submission:	Final Report
Inst. Control Number:	FA9550-06-1-0045P00001
Institution:	UNIVERSITY OF TEXAS AT DALLAS
Primary Investigator:	Dr. Bhavani Thuraisingham
Invention Ind:	none
Project/Task:	2311F / X
Program Manager:	Robert L. Herklotz

Objective:

There is a critical need for organizations to share data within and across infospheres and form coalitions so that analysts could examine the data, mine the data, and make effective decisions. Each organization could share information within its infosphere. An infosphere may consist of the data, applications and services that are needed for its operation. Organizations may share data with one another across what is called a global infosphere that spans multiple infospheres. It is critical that the war fighters get timely information. Furthermore, secure data and information sharing is an important requirement. The challenge is for data processing techniques to meet timing constraints and at the same time ensure that security is maintained. This proposal addresses information operations across infospheres. It first describes secure timely data sharing across infospheres and then focus on Role-based access control and Usage control in such an environment. The goal is to send timely information to the war fighter while maintaining security. It will also address the application of game theory as well as decision centric data mining techniques to extract information from both trustworthy and untrustworthy partners of the coalition. In particular, the objectives of this project are as follows:
o Develop a Framework for Secure and Timely Data Sharing across Infospheres.
o Investigate Access Control and Usage Control policies for Secure Data Sharing.
o Develop innovative techniques for extracting information from trustworthy and untrustworthy partners.

Approach:

This grant proposes a collaborative approach for secure timely data sharing where data, metadata, and policies are exported and integrated at the coalition level. It will develop approaches to mine the data in a collaborative peer-to-peer environment and examine the security impact. It will also develop techniques for enforcing security policies. In particular,it will focus on two of the most prominent policies: role-based policies and usage control policies. The enemy organization may want to infiltrate our organization and find out more about its activities. In such cases, we not only have to extract information from the adversary, but we must also protect our data and activities. While this is a very challenging problem, we need to start research in this area. Therefore this project will also address applications of game theoretic and decision centric data mining techniques to extract information across the infospheres.

Progress:

DTIC Data

Progress:

Year: 2006 **Month:** 10

We have proposed three models for information sharing across organizations. In the first model, the partners of the coalition are considered to be trustworthy. In the second model, the partners are semi-trustworthy. In the third model the partners are untrustworthy. We need to consider all three models in order to fight the global war on terror. For each model, we need to apply different techniques for sharing data and extracting information. Our research investigates the various approaches for assured information sharing.

Year: 2007 **Month:** 12

We have examined three models: In the first model the
partners of the coalition are considered to be trustworthy. In the second model, the partners are semi-trustworthy. In the third model the partners are untrustworthy.

The report essentially consists of three four parts; three of which are produced by members of the UTD team and one is produced by members at GMU (now UTSA) team. We first provide an introduction to the project as well as the developments during Year 2. This introduction was also presented at the AFOSR review in June 2007. In the case of trustworthy models we conducted experiments on data sharing vs. data policy enforcement and developed a prototype systems based on the concepts developed during Year 1. This work is published as a UTD Technical Report (Pa rt 1). For the temitrustworthy model we examined the use of game theory for extracting information from the partners. We enhanced the research carried out during Year 2. This research is
published in a UTD Technical Report (Part II). For the untrustworthy model, we examined the use of data mining for defensive operations. This research is published in a UTD Technical Report (Part III).

In addition to the above, George Mason University (GMU) received a subcontract from the University of Texas at Dallas to examine the use of Role-based Access Control (RBAC) and Usage Control models for Coalition data sharing. The research was carried out at GMU between January and May 2007. This research is in the form of a presentation and is included in the report (Part IV). This subcontract has now moved to the University of Texas at San Antonio (UTSA) since the PI has moved to UTSA from GMU.

Year: 2009 **Month:** 11

The research reported in this annual report was carried out mainly at the University of Texas at Dallas (UTD) between December 1, 2007 and November 30, 2008. It describes the issues and challenges for information operations across infospheres and focuses on assured information sharing. We have examined three models: In the first model the partners of the coalition are considered to be trustworthy. In the second model, the partners are semi-trustworthy. In the third model the partners are untrustworthy.

Year: 2009 **Month:** 10 **Final**

There is a critical need for organizations to share data within and across infospheres and form coalitions so that analysts could examine the data, mine the data, and make effective
decisions. Each organization could share information within its infosphere. An infosphere may consist of the data, applications and services that are needed for its operation.
Organizations may share data with one another across what is called a global infosphere that spans multiple infospheres. It is critical that the war fighters get timely information.
Furthermore, secure data and information sharing is an important requirement. The challenge is for data processing techniques to meet timing constraints and at the same time ensure that security is maintained

Information Operations Across Infospheres

FINAL REPORT

Prepared by

The University of Texas at Dallas

Submitted to:
Air Force Office of Scientific Research

November 30, 2008

Under
Contract: FA9550-06-1-0045

Period of Performance:
December 1, 2005 – November 30, 2008

Subcontractor:
The University of Texas
at San Antonio

EXECUTIVE SUMMARY OF PROJECT

Therc is a eritieal need for organizations to share data within and aeross infospheres and form eoalitions so that analysts eould examine the data, mine the data, and make effective decisions. Eaeh organization could share information within its infosphcre. An infosphere may consist of the data, applications and services that are needed for its operation. Organizations may share data with one another aeross what is ealled a global infosphere that spans multiple infospheres. It is eritieal that the war fighters get timely information. Furthermore, secure data and information sharing is an important requirement. The ehallenge is for data processing techniques to meet timing eonstraints and at the same time ensure that security is maintained.

This proposal addresses information operations across infospheres. We first dcscribe seeure timely data sharing across infospheres and then focus on Role-based aecess control and Usage control in such an environment. Our goal is to send timely information to the war fighter while maintaining security. We will also addrcss the application of game theory as well as decision eentrie data mining teehniqucs to extraet information from both trustworthy and untrustworthy partners of the coalition.

In particular, the **objectives** of this project are as follows:

- Develop a Framework for Seeure and Timely Data Sharing aeross Infospheres.
- Investigate Access Control and Usage Control policies for Securc Data Sharing.
- Develop innovative techniques for extracting information from trustworthy and untrustworthy partners.

Technical Merit: While there has been work on data sharing aeross coalitions, an in-depth investigation of seeurity issues as well as a study of the tradeoffs between seeurity and timely proeessing has yet to be earried out. To our knowledge, this projeet is the first to investigate sophistieated seeurity teehniques such as Usage Control as well as deeision eentrie data mining teehniques for timely and seeure data sharing aeross eoalitions.

Broader Impact: The rescarch to be carried out on this project is directly applicable to Network Centric Operations (NCO) that implement Network Centric Warfare (NCW). NCW promotes information sharing, shared situational awareness and knowledge of eommander's intent. In addition it also enables war fighting advantage by providing synchronization, speed of eommand and inereased eombat power. We foeus mainly on information sharing aspects of NCW. In particular, the results of this project can be transferred to the timely and seeure data sharing serviees of the Network Centric Services aetivity being earried out by the Department of Defense.

Research Team: The researeh will be earried out both at the University of Texas at Dallas and at George Mason University. The prineipal investigators are among the leading rescarchers in Data and Applications Security. They have conducted innovative researeh in Seeure Database Design, the Inferenee Problem, Role-based Aeeess Control and Usage Control techniques as well as and carried out technology transfer activities. They are Fellows of IEEE, ACM, AAAS and the British Computer Soeiety and have received prestigious awards for their research in Data and Applieations Security.

ABSTRACT OF FINAL REPORT

The research reported in this final report was carried out mainly at the University of Texas at Dallas (UTD) between December 1, 2005 and November 30, 2008. It describes the issues and challenges for information operations across infospheres and focuses on assured information sharing. We have examined three models: In the first model the partners of the coalition are considered to be trustworthy. In the second model, the partners are semi-trustworthy. In the third model the partners are untrustworthy.

George Mason University (GMU) received a subcontract from the University of Texas at Dallas to examine the use of Role-based Access Control (RBAC) and Usage Control models for Coalition data sharing. The PI moved to UTSA and received the next phase of the funding to work on group-based information sharing (Part 1).

ACKNOWLEDGEMENT

Much of the research discussed in this annual report was supported buy the Air Force office of Scientific Office under Contract FA9550-06-1-0045. We thank Dr. Robert Herklotz of AFOSR for funding his encouragement and motivation. This research as also partially supported by the Erik Jonsson School of Engineering and Computer Science at the University of Texas at Dallas under the Texas Enterprise Funds. We thank Prof. Mark Spong (Dean) for this support.

SUMMARY

1. Problem and Objectives

There is a critical need for organizations to share data within and across infospheres and form coalitions so that analysts could examine the data, mine the data, and make effective decisions. Each organization could share information within its infosphere. An infosphere may consist of the data, applications and services that are needed for its operation. Organizations may share data with one another across what is called a global infosphere that spans multiple infospheres. It is critical that the war fighters get timely information. Furthermore, secure data and information sharing is an important requirement. The challenge is for data processing techniques to meet timing constraints and at the same time ensure that security is maintained.

This proposal addresses information operations across infospheres. We first describe secure timely data sharing across infospheres and then focus on Role-based access control and Usage control in such an environment. Our goal is to send timely information to the war fighter while maintaining security. We will also address the application of game theory as well as decision centric data mining techniques to extract information from both trustworthy and untrustworthy partners of the coalition.

In particular, the **objectives** of this project are as follows:

- Develop a Framework for Secure and Timely Data Sharing across Infospheres.
- Investigate Access Control and Usage Control policies for Secure Data Sharing.
- Develop innovative techniques for extracting information from trustworthy and untrustworthy partners.

2. Our Approach

We developed three classes of solutions to handle the different types of partners. For trustworthy partners we developed solutions for policy based information sharing. For semi-trustworthy partners we applied game theoretic techniques to extract as much information as possible from the partners. For untrustworthy partners we protected our systems by providing solutions to malicious code detection. In addition, we also designed an approach to carry out active defensive (i.e. offensive) operations.

3. Our Contributions

This is the final report for the project. The contents of this report describe our research during Year 3. In this section we discuss our solutions for handling all three types of partners and mention the contributions during each year.

To handle trustworthy partners we first determined the amount of information that is lost when policies are enforced (report 1). We introduced the notion of release factor and showed that the amount of information lost decreases with release factor. We also conducted simulation experiments for policy based information sharing (report 1). Next we developed a proof of concept prototype that demonstrated policy based information sharing. We utilized medical databases and applications (report 2). In addition we also developed an approach to assign trusts levels to the partners in a peer to peer information sharing environment (report 2). Finally our subcontractor (initially at GMU and then at UTSA) has developed the idea of group-based information sharing where documents as well as members join and leave the coalition. The usage control model was extended to a group-based environment (report 3 – that is, this report).

To handle semi-trustworthy partners, we explored game theoretic techniques. Our goal is to extract as much information as possible from out partners and not divulge any of our information. During the first two years we conducted simulation studies using various types of games (report 1 and report 2). During Year 3 we applied the techniques to a bioterrorism attack (report 3). The goal of our work was to apply proven human-oriented situation analysis with existing simulation techniques to explore new ways of enhancing security through anticipation of human thought processes and activity. In particular, we used social networking to model relationships and game theory to model motivations of those participating. The end result of these studies yielded a combination of methods to anticipate, plan for, and reduce the impact of a biological attack. The SIR model was modified and applied to an individual-level social network through the use of theatres and approximated influences due to relationships, creating a unique, high performance mathematical model to observe the spread of disease. This model was then simulated in a number of scenarios spanning the use of possible attack situations, inoculations, and several novel intervention methods. The results of the simulation were then analyzed as a Stackelberg game in order to search for a lower bound to the expected costs and loss of human life under the assumption that the attacker goes last.

To handle untrustworthy partners we explored mainly defensive operations. Here we applied data mining techniques for malicious code detection (report 1 and report 2). During Year 3 we continued to apply data mining techniques for botnet detection (report 3). In addition we also designed techniques for offensive operations where the viruses that we develop will change patterns when new patches are introduced (report 3). We propose to enhance the design in our follow-on proposal that will focus on offensive operations.

3. Significant Outcomes

The total budget for this project is 300K from AFOSR and 150K in matching funds from the State of Texas. (i) One significant outcome of our research is the one pager we submitted to AFOSR on assured information sharing. This one pager was released as a MURI BAA in 2007 and subsequently AFOSR has made two multimillion dollar awards. (ii) We have also made presentations of our results to various air force bases through AFCEA including Edwards AFB and Kirkland AFB in 2006. (iii) We have also presented our research to other agencies and now have contracts and grants with NGA for geospatial semantic web and with IARPA to solve challenging problems in semantic web. (iv) We have published several papers in high quality journals and conferences and

have given keynote addresses including at the IEEE Intelligence and Security Informatics Conference in 2008. (iv) Finally this research has developed a new area in data and applications security and that is on inventive based information sharing. We will further develop these ideas under our MURI project.

4. Impact on Theses and Education

This project had a major impact on MS/PhD degrees and courses. The research has provided support for the PhD Thesis research of Ryan Layfield who has successfully defended his thesis (graduation December 2008) on applying game theory for information sharing (report 3). Ryan started his PhD work in the Spring of 2005 just before this project began. In addition it has also supported the PhD Thesis of Mehedy Masud on Data Mining for Cyber Security Applications (to graduate in 2009). Nathalie Tsybulnik was partially supported by this project for her PhD to develop techniques for assigning trust levels in a peer to peer environment. A PhD student at GMU/UTSA was also supported by this project on group-based information sharing. Several MS students have contributed to the programming projects. In particular Yashaswini Harshakumar developed the prototype for policy based information sharing Dilsad Cavus worked on examining the amount of information that is lost by enforcing policies. Srinivas developed simulation experiments on assured information sharing.

Mamoun Awad, a post-doctoral researcher was particularly supported by the project to supervise the experiments carried out during the first year of the project. The professors who have advised the students are: Bhavani Thuraisingham, Latifur Khan, Murat Kantarcioglu and Kevin Hamlen at UTD and Ravi Sandhu at UTSA.

In addition to incorporating units on information sharing to courses taught at AFCEA, we are also introducing a new graduate level course on data mining for cyber security applications. We have incorporated several units based on this research to our course in data and applications security.

5. Organization of the Reports.

The technical work has been described in three annual reports submitted to AFOSR in October 2006, November 2007 and November 2008.