NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

AN ARCHITECTURE FOR NETWORK CENTRIC OPERATIONS IN UNCONVENTIONAL CRISIS: LESSONS LEARNT FROM SINGAPORE'S SARS EXPERIENCE

by

Chee Bin, Tay
Whye Kee, Mui

December 2004

Thesis Advisor:	Gurminder Singh
Second Reader:	Arijit Das

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2004	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE: An Architecture for Network Centric Operations In Unconventional Crisis: Lessons Learnt from Singapore's SARS Experience.

5. FUNDING NUMBERS

6. AUTHOR(S) Chee Bin, Tay and Whye Kee, Mui

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Office of Force Transformation, DoD US
Future Systems Directorate, MINDEF Singapore

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

Singapore and many parts of Asia were hit with Severe Acute Respiratory Syndrome (SARS) in March 2003. The spread of SARS lead to a rapidly deteriorating and chaotic situation. Because SARS was a new infection, there was no prior knowledge that could be referenced to tackle such a complex, unknown and rapidly changing problem. Fortunately, through sound measures coupled with good leadership, quick action and inter-agency cooperation, the situation was quickly brought under control.

This thesis uses the SARS incident as a case study to identify a set of network centric warfare methodologies and technologies that can be leveraged to facilitate the understanding and management of complex and rapidly changing situations. The same set of methodologies and technologies can also be selectively reused and extended to handle other situations in asymmetric and unconventional warfare.

.

14. SUBJECT TERMS
Network Centric Warfare, Technical Architecture, Mobile Computing, Collaborative Networks, Social Networks, Networks, Data Interoperability, Middleware, Ad hoc Processes, Ad Hoc Teams

15. NUMBER OF PAGES
101

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

THIS PAGE INTENTIONALLY LEFT BLANK

AN ARCHITECTURE FOR NETWORK CENTRIC OPERATIONS IN UNCONVENTIONAL CRISIS: LESSONS LEARNT FROM SINGAPORE'S SARS EXPERIENCE

Chee Bin Tay
Lieutenant Colonel, Republic of Singapore Army
B.Sc (Computer Science), National University of Singapore, 1989

Whye Kee Mui
Civilian, Defence Science and Technology Agency, Singapore
B.Sc (Computer Science), National University of Singapore, 1993

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
December 2004

Author:	Chee Bin Tay Whye Kee Mui
Approved by:	Gurminder Singh Thesis Advisor
	Arijit Das Second Reader
	Peter Denning Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Singapore and many parts of Asia were hit with Severe Acute Respiratory Syndrome (SARS) in March 2003. The spread of SARS lead to a rapidly deteriorating and chaotic situation. Because SARS was a new infection, there was no prior knowledge that could be referenced to tackle such a complex, unknown and rapidly changing problem. Fortunately, through sound measures coupled with good leadership, quick action and inter-agency cooperation, the situation was quickly brought under control.

This thesis uses the SARS incident as a case study to identify a set of network centric warfare methodologies and technologies that can be leveraged to facilitate the understanding and management of complex and rapidly changing situations. The same set of methodologies and technologies can also be selectively reused and extended to handle other situations in asymmetric and unconventional warfare.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1

A. BACKGROUND 1

1. The SARS Incident in Singapore – An Unconventional War Scenario 1

2. Fight against SARS 2

B. NETWORK CENTRIC WARFARE AND SARS 4

1. Network Centric Warfare Framework in a Non-Military Setting 4

2. Fight against SARS and Network Centric Warfare 5

C. NCW LESSONS FROM SARS 7

1. Information Sharing 8

2. Ad Hoc and Flexible Organizational Structure 8

3. Inter-Agency Processes 8

4. Mobility and Agility 9

5. Employment of Technology 9

D. CLASSES OF ACTORS AND THEIR INFORMATION NEEDS FOR DEALING WITH UNFAMILIAR CRISIS 9

1. Classes of Actors 9

a. Strategic Decision Makers 10

b. Operations Coordinator 10

c. Mobile Executor 11

d. Content Managers 11

2. Information Needs 11

a. Abstract Information 12

b. Executive Information 12

c. Specific Information 12

E. TECHNICAL ARCHITECTURE TO SUPPORT NETWORK CENTRIC OPERATIONS IN UNCONVENTIONAL CRISIS 13

1. Cardinal Requirement and Support Technology 13

a. Data Interoperability 13

b. Support for Ad Hoc Structure 14

c. Support for Mobility 15
F. THESIS OUTLINE 15

II. NETWORK CENTRIC WARFARE 17
A. IMPETUS FOR NETWORK CENTRIC WARFARE 17
1. Emerging Challenges 17
a. Unpredictable Global Politics 17
b. Terrorist and Insurgence Threats 18
2. Changing Environment 18
a. Advances in IT Capability 19
b. Connectivity, Portability and Mobility 20
c. Globalization 20
B. ARMED FORCES RESPONSE TO THE CHANGING ENVIRONMENT 21
C. TENETS OF NETWORK CENTRIC WARFARE 22
D. DOMAINS OF NCW 24
1. Cognitive Domain and Social Domain 24
2. Physical Domain and Information Domain 25

III. NETWORK CENTRICITY IN SINGAPORE’S FIGHT AGAINST SARS 27
A. SARS INCIDENT IN SINGAPORE 27
1. Early Stage of the Outbreak 27
2. Deterioration of the Situation 29
3. Intertwined Scale-Free Network of Problems 30
B. SOCIAL AND COGNITIVE DOMAIN OF THE SARS BATTLE 32
1. Recognizing That There Will be a Problem 32
2. Collaborative Group Decision Making and Consensus Building 33
3. Scoping the Problem and Determining the Solution 33
C. INFORMATION AND PHYSICAL DOMAIN OF THE SARS BATTLE 34
1. Changes in Organization and Processes 34
2. Collaboration, Decision Making Process and Share Vision 36
3. Multi Agencies Processes and Executions 37
4. Information Sharing 38

5. Employment of Technology 40
D. THE GLOBAL BATTLE 40
E. LESSONS LEARNT 41
IV. REQUIREMENT FOR NETWORK CENTRIC OPERATIONS 43
A. INTRODUCTION 43
B. BACKGROUND AND BROAD REQUIREMENTS 43
1. Key Challenges Involved 45
C. KEY CONSIDERATIONS 45
D. USERS OF THE SYSTEM 46
1. Decision Makers 47
2. Operations Coordinators 47
3. Mobile Executers 48
4. Content Managers 48
V. TECHNICAL ARCHITECTURE TO SUPPORT NETWORK CENTRIC OPERATIONS FOR UNCONVENTIONAL CRISIS 49
A. ARCHITECTURE FOR UNCONVENTIONAL CRISIS 49
B. UNIFIED INFORMATION BUS 51
C. DATA INTEROPERABILITY 51
1. Identify the Information Requirement for the Mission 52
2. Identify the Data Sources to Fulfill the Requirement 52
3. Identify the Information Needs for the Different Roles of a Mission 53
4. Retrieval of the Data Sources 54
5. Processing of the Retrieved Data Sources 54
D. TOOLS TO ENABLE DATA INTEROPERABILITY 54
1. Meta-data Management Tools 55
2. Middleware 56
a. Transactional Middleware 57
b. Message-Oriented Middleware 57
c. Procedural Middleware 57
d. Object and Component Middleware 57
e. Enterprise Application Integration Middleware 58
f. Web Services Middleware & XML 58
3. Data Processing Tools 60

4. An Example of Data Interoperability Solution 61

E. ENABLING AD-HOC TEAMS 61

1. Situation Collation Manager 61

2. Information Dissemination Manager 62

3. Information Update Tracker 62

4. Access Control Manager 62

5. Search and Query Manager 63

6. Dynamic Process Manager 64

7. Event Alert Manager 64

8. Collaboration Tools 65

9. Analysis & Simulation Tools 66

F. SUPPORT FOR MOBILE COMPUTING 67

1. Mobile Gateway Module 67

2. Priority Information Alert Service 68

3. Mapping Information Services 68

4. Mobile Reporting Module 68

5. Infrastructure for Mobile Communication 69

G. CONCLUSION 71

VI. CONCLUSION AND FUTURE WORK 73

A. CONCLUSION 73

B. ENHANCEMENTS TO THE TECHNICAL ARCHITECTURE 74

1. Service Oriented Architecture 74

2. Security Services 75

3. Information Exploitation Services 75

4. Information Presentation Services 76

5. Mobile Computing Services 76

C. EXPLORATION ON COGNITIVE SERVICES 77

1. Analysis Tools 77

2. Hypothesis Tools 78

D. SIGNIFICANCE OF THE SOCIAL NETWORKS 78

BIBLIOGRAPHY 81

INITIAL DISTRIBUTION LIST 85

LIST OF FIGURES

Figure 1. Four Different Classes of Actors of Users to be Supported 10
Figure 2. Moore’s Law [www.intel.com/research/silicon/mooreslaw.htm, 2004] 19
Figure 3. NCO Domain [John & Albert, Jun 2004] 24
Figure 4. Early Stage of the Outbreak 28
Figure 5. Non Linear, Complex System.. 29
Figure 6. Intertwined Network of Problems... 31
Figure 7. Organizational Structure for Fight Against SARS 35
Figure 8. Information for Contact Tracing 39
Figure 9. Four Different Classes of Users to be Supported. 47
Figure 10. Technical Architecture For Unconventional Crisis. 50
Figure 11. Example of using Link Analysis Tool to trace the SARS Infection 66
Figure 12. Example of Wireless Metropolitan Area Network. [Cisco].................. 70

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would to thank our advisors, Professor Singh and Professor Arijit Das for their patience, guidance and advise throughout the process. We would like to thank Professor Susan Higgins for her valuable inputs and insights. We also like to thank BG Jimmy Khoo and Mr. John J. Garstka for this opportunity to work on such an interesting subject. We would like to express our gratuity to our friends for their value inputs.

Special thanks to our families for their support and kind understanding throughout this demanding period.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

1. The SARS Incident in Singapore – An Unconventional War Scenario

Between February 20 to 25 2003, three Singaporean women traveled to Hong Kong and contacted a mysterious pneumonia-like fever which was later diagnosed as Severe Acute Respiratory Syndrome (SARS). Around the same time, the rumors of the spread of a similar disease had also been received from Southern China. Given the nature of the virus, the Singapore government concluded that they have a highly infectious disease outbreak at hand and recommended that the patients be isolated [Chua Mui Hoong, 2004]. It was the correct thing to do, but by the time this action was taken, it was too late. The virus began to spread rapidly and several others had already been infected with SARS. The SARS incident in Singapore not only affected the health community but also had social psychological and economical fallouts.

Little was known about this new disease at that time. Unknowns included the cause of the disease, the symptoms a SARS patient, how the disease is transmitted and the incubation period before a SARS patient will show signs of infection. These unknown created fear within the general public and health workers. Stopgap measures were being developed as pieces of new information were discovered.

Soon the battle was no longer confined to just another infectious disease incident. Among other factors, lack of knowledge about the virus, metropolitan nature of Singapore and Singapore’s position as one of the global transportation hub soon drew other sectors of the nation into this incident. The interplay between various aspects of the incident and constant bombardment of discovery of new facts was unprecedented. In many respects, it was like fighting an unconventional war where the enemy is elusive, and the battle is raging on within populated areas where civil-military operations had to be managed and ‘collateral’ damages minimized.

The pressure was reduced after three grueling months of battling with the disease when WHO took Singapore off the SARS list. Removal from SARS watch list relieved pressure off the economic, travel and social-psychological front. However, Singapore continued to enhance her defenses against the virus as no one can could tell when the enemy will strike again.

2. Fight against SARS

During the initial unsuspecting stage, medical professionals in Singapore were confident that SARS could be easily contained. All indicators pointed to a standard infectious disease control situation. Government reassured the public that there was no cause for alarm. There were little warnings as to the looming crisis which was about to occur.

Within a short span of 2 weeks, the situation in Singapore deteriorated rapidly. The media reports of the unknown virus and seepage of the virus from Tan Tock Seng Hospital (TTSH) to Singapore General Hospital (SGH) generated widespread fear and anxiety. The public was seized by fear, travelers shunned Singapore and the nation was slowing grinding to a halt.

Given the seriousness of the situation, the government decided to tackle it on a war footing. With the declaration of war, full machinery of the government and quasi-government agencies swung into action. The spread of the virus was to be halted, public fear be allayed and world’s confidence in Singapore be restored.

To achieve these, Singapore initiated several rather strict measures. These included home quarantine orders for anyone who came in contact with patients suspected to be infected with SARS, strict border control to prevent the export of possible SARS cases to other countries and eliminate further introduction of SARS cases into Singapore, effective contact tracing system to determine who came in contact with SARS infected patient and the designation of dedicated SARS hospital to provide the focal point in the battle plan.

These measures were essential and effective in controlling the spread of the disease. The progress instilled public confidence and the trust in the government. With this confidence, people became comfortable to move out of the house and lead their life normally.

Most of these measures pioneered by Singapore were rapidly adopted by many other countries or cities to fight SARS. But no countries executed these measures as well as Singapore did, as noted by WHO observers Dr David Heymann, Dr Mansoor and Dr Lambert during their separate observation missions to Singapore during the crisis – “whatever Singapore did, it did it faster and more thoroughly”.

However, questions still loom: How did Singapore execute all the new control measures with such effectiveness and efficiency? How the SARS fighting machinery was able to adapt itself to the changing scenario rapidly? What helped the formulation of these pioneering control measures?

The overall success was attributed to effective communication between the government and the people, strong leadership, people’s cooperation and inspired healthcare workers. Several studies, analysis and interviews had also been conducted focusing on information management, public communication, medical readiness and medical research.

As we probe deeper into Singapore’s fight against SARS, we discover that at the heart of the fight was much about information. It involved knowing what information is important; where and how to get it. It was also very much about how the various agencies evolving themselves around the collection, processing, analysis and use of information. It was also about how information is shared with the public.

Beside exploitation of information, Singapore’s fight against the SARS disease also exemplified Network Centric Warfare (NCW) concepts in many aspects. NCW has been discussed predominately within military context. Nonetheless, several key NCW concepts were present in the fight and the episode serves as an excellent case study of NCW being employed in a non-military setting.

B. NETWORK CENTRIC WARFARE AND SARS

1. Network Centric Warfare Framework in a Non-Military Setting

So far much of the discussion of NCW has been focused in the military context. The impetus for NCW has been to adapt conventional armed forces to be in line with the new global era and information age. The primary aim is to increase combat effectiveness of forces in traditional missions and to counter new threats where traditional approaches may not effective.

Literature search reveals that there are multiple definitions to NCW. In [Alberts, Garskta, Stein 2000], NCW is defined as “an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace.”

Key NCW concepts include

- Changes in the organizations and processes to improve their efficiency and effectiveness.
- Networking people through the use of information technologies to enable virtual integration, information sharing, improve sensing and response, enable collaboration and synchronization.
- Making nodes and people network ready, so that they are more effective in collaboration and sense making.

NCW principles and concepts can be adapted or applied in non-military setting. Corporations are re-structuring themselves and their processes to improve information flow and decision-making. Government agencies are linking up, enhancing information exchanges and reaching out to citizen to provide better services and governance.

Adoption of NCW concepts can be seen in the fight against SARS in Singapore. The tempo, uncertainty, and unconventional nature of the crisis make it an unusual opportunity to validate NCW concepts being employed in unconventional scenario.

2. Fight against SARS and Network Centric Warfare

The SARS crisis started in Singapore seemingly as a standard infectious disease containment problem. Singapore has been well prepared for such incidents involving infectious diseases. Standard Operating Procedures (SOP) were developed and refined over the years for incidents such as the polio outbreak in the 1958 and the Nipah virus incident in Malaysia in 1999 with isolated cases in Singapore. However, what differentiated SARS from other contagious diseases was that very little was known about this new disease. This negated the effectiveness of the various established SOPs. The medical community did not know what it was that they are trying to contain.

The ignorance created fear, anxiety and the spillage to other aspects of the nation increased the complexity of problem dramatically. The disease had effectively opened up several other battlefronts in its campaign. Ad hoc measures were implemented with limited information and danger of repercussion to other aspects. The measures challenged the traditional governmental hierarchy and stove-piped structure. Not only inter-ministries interactions were required, they were expected to happen in near real time as the situation changed and new findings on the virus are found.

To affect the control measures effectively, ad hoc structures and processes which spanned agencies were established. Furthermore, these ad hoc structures, processes and people had to constantly adapt as the situation evolved and new information were received. A great amount of agility was featured during the fight.

Media coverage and the Internet increased the tempo and complexity of the episode. New occurrences, infectious count, travel warnings and advisories were broadcast in near real time. Interpretation and speculation raged on in the cyber world and in “coffee shop”[1]. Government actions needed to be responsive to maintain the confidence and trust of the people. Failing which, public speculation, suspicion and fear could have spiraled out of control.

Throughout the fight, information technologies were employed extensively. Organizational barriers were torn down and inter-agency processes established whenever required. Information flowed freely; decisions were made collectively which resulted in all agencies not only understanding the decisions but also the intent and rationale behind those decisions. This enabled each agency to senses, respond and seek out more relevant information own their own; achieving a certain degree of synchronization. Decision makers formed coherent pictures out of a chaotic and unfamiliar situation and navigated from the unknown to knowable.

We detected several aspects of NCW being employed in the fight against SARS. We are also sure that the employment of NCW concepts was not a conscious guiding principle in the fight against SARS. It seems that some unspoken cultural norm amongst the various agencies, coupled with the common objective of bringing this fight to an end as quickly as possible, was sufficient for inter-agency processes to developed; information to flow freely across agencies; decision makers and frontline workers alike recognized the importance of timely and accurate information. This subconscious cultural norm is perhaps also partly due to the affluence of Singapore whereby information and technology is a nature aspect of the society. However, the focus of this thesis is not what resulted in NCW being featured in SARS. The questions we will attempt to

[1] Common local dinning place in Singapore

answer are: How much do employment of these concepts contributed to the success of Singapore in combating the SARS disease? What can we learn from this episode? How can we better prepare ourselves for such unconventional, unknown and asymmetric scenarios?

To answer these questions, this thesis analyzes significant events throughout the fight against SARS in Singapore, decisions and actions taken during those events. From the analysis, we will draw out lessons from this episode. We will then attempt to generalize these lessons learnt to be applicable in similar situations in Singapore and elsewhere. We will also propose a technical architecture to facilitate the exchange and exploitation of information, and creation of ad hoc structures and processes which are the critical success factors in dealing with unconventional crisis such as SARS.

C. NCW LESSONS FROM SARS

As observed by WHO, what differentiated Singapore from other SARS affected countries were the speed and thoroughness in which the various control measures were executed. It is also recognized that despite the lack of knowledge about the new virus and the rapid changing environment, Singapore was able to identify key problem areas and develop new and effective measures faster and better than other countries. Analyzing the various key events, and decisions which took place, we determined the primary factor was that Singapore exploited information better than others. Singapore was able to ensure timely distribution of information for collaboration, decision-making, execution and feedback. The other factor was the flexibility and agility in which Singapore organized itself to tackle the various situations. These two factors manifested in the various strengths identified:

1. Information Sharing

The Singapore government agencies were able to identify quickly what information was needed and its sources. They were able to develop processes, either manual or computerized, to ensure the timely collection and distribution of information. For example, the contact-tracing center was linked to civilian telephone directory services, National Registration Office, Ministry of Manpower database. This increased the efficiency of the contact tracing. The Home Quarantine Order (HQO) information was pushed to border control on a timely basis to prevent people served with HQO from leaving the countries.

2. Ad Hoc and Flexible Organizational Structure

Most of the control measures implemented required numerous organization and agencies to work in synchronization. These included the execution of Home Quarantine Orders, creation of a “SARS free corridor”, perception management and labor market management. The containment of a community outbreak in the Pasir Panjang Wholesale Centre (PPWC)[2] proved to be a major challenge in the entire SARS episode. Multiple agencies were pulled together to contain the outbreak and its various other fallouts.

These demonstrated the need and effectiveness of ad hoc structure needed to deal with unknown situations. Agility of these ad hoc structures to evolve as situations changed was another strength demonstrated by Singapore. It was able to bring different agencies and expertise together, enabling collaboration and enhancing the decision making process.

3. Inter-Agency Processes

Beside the enhanced collaborations and decision-makings, Singapore government agencies also demonstrated the ability to implement and execute

[2] The primary vegetable and fruits produce whole sale centre in Singapore. It imports 80% of Singapore’s daily fresh produces consumption needs.

complex measures and activities involving multi-agencies. This ability was key to the speed, thoroughness and effectiveness demonstrated.

However, some gaps and lapses in these inter-agency processes also resulted in the spreading of SARS into SGH, and PPWC. We identified that this is one of the areas in which technology can help to enhance the execution of inter-agency processes.

4. Mobility and Agility

Information was available for the ground executors. However, the means used were rudimentary such as cellular (or hand) phones and communication sets such as walkie-talkies. While this did not result in any significant setbacks in the fight, the efficiency of the ground executors could have been improved with enhanced information services. These ground executors could have acted as sensors and provided timely feedback.

5. Employment of Technology

During the early stage of the crisis, most of the activities were human intensive. This had resulted in gaps and mistakes. Technologies, especially information technologies were introduced when the situation spiraled into a crisis. Due to limited time, technologies were employed only in contact tracing, hospital movement and border control. However, these were sufficient to demonstrate the increased in effectiveness brought about by technology.

D. CLASSES OF ACTORS AND THEIR INFORMATION NEEDS FOR DEALING WITH UNFAMILIAR CRISIS

1. Classes of Actors

Using Singapore's SARS incident as a case study, we identified 4 main classes of actors. We assessed that classes of actors dealing with unfamiliar crisis can be generalized to the following:

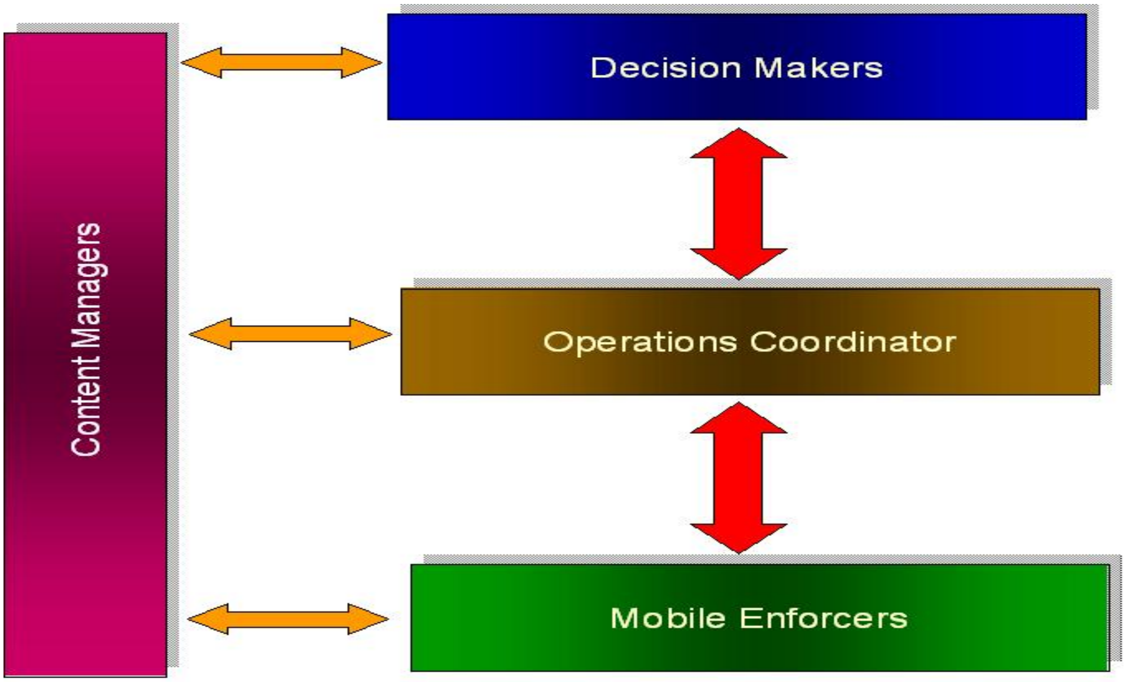

Figure 1. Four Different Classes of Actors of Users to be Supported

a. *Strategic Decision Makers*

Strategic decision makers perceive the problem, formulate alternatives and decide the courses of action. In many cases, they make decisions with incomplete information, make judgments, and decide on hunches or rational choices with constraints. Their information needs range from represented data in computers systems to un-captured information such as conversation, sentiments, media broadcast and tacit wisdom. They rely heavily on what we call the abstract class of information and to a large extend executive information.

b. *Operations Coordinator*

Operations coordinator translates decisions into action plans. To do that, they need to understand the intent of the decisions and the context in which the decisions were made. They will chart out the activities required, sequence and synchronizes activities across functional groups. They need to monitor the progress and the trends of the environment and make adjustments if necessary. Their information needs are primarily feedbacks, trends, statistics and reports.

c. Mobile Executor

Mobile executors execute tasks and orders and are in direct contact with events happening on the ground. Their primary information needs are highly specific and are related to their task and their immediate operating environment. Though their effectiveness may be enhanced with more information, beyond a point, the increase is marginal and there is a possibility of information overload. Mobile executors are excellent sensors as they are directly in contact with the situation in real time.

d. Content Managers

While not directly involved in actions, the content managers' role is perhaps the most critical. They are required to understand the essences of decisions and processes and determine the information sources needed to support these. They need to ensure that the information sources are compatible at various levels so that the information will not be used out of context. Content managers also need to ensure the packaging and the presentation of information helps the entire operations. They are to determine if there are uncertainties within the information provided and explain how the uncertainties may affect decisions and actions.

2. Information Needs

Depending on their roles, actors within a crisis need different mix of information of different nature. We classified the information needs into 3 general classes:

a. Abstract Information

Information in this class is mostly tacit in nature. This includes cognitive information such as wisdom, imagination, experience, metaphor or complex cause-effect relationship. Given the short observation duration of crisis and the interplay of multiple factors, it is not immediately obvious the relationship between information entities. The cause-effect relationship of actions and observed environment also cannot be established with certainty within the short observation duration.

It is generally difficult to map information within this class. This is especially so given the time constraints and the differences in the interplay of factors in each situation.

b. Executive Information

Executive information is higher level interpretation of specific information. This includes trends, relationships and deviations of groups of specific information. These analyses can further be used to develop models and hypotheses of the situation. Assumptions and estimates can be made with varying degree of uncertainty to fill in the information gaps. Optimization with constraints, modeling and simulation can be carried to generate possible courses of action.

While executive information may be complex in form or presentation, it can be represented and represent the knowable. Information in this class are used for decision making in complex but mostly known situations.

c. Specific Information

Information in this class is necessary for the completion of a task such as *deliver* item X to *person* Y in *location* Z by *time* H or in the analysis of trends such as *number* of *people* with *symptom* in this *area*. This information exhibits high degree of certainty and can be represented, stored, manipulated, queried and transmitted.

E. TECHNICAL ARCHITECTURE TO SUPPORT NETWORK CENTRIC OPERATIONS IN UNCONVENTIONAL CRISIS

1. Cardinal Requirement and Support Technology

Using Singapore's SARS incident as a case study, we determined the various NCW concepts that were employed and the improvement in operational efficiency achieved. We also identified limitations of executing newly established inter-agency processes manually and the data interoperability issues associated in briefing ad hoc people and systems together. From the case study, we determined that appropriate application of information technology will complement the application of NCW concepts. The main challenge is the integration of the various technologies into a large-scale system. From the lessons learnt from SARS, the roles of various classes of actors and their information needs, we identified the following cardinal requirement, support technology and the architecture for this system:

a. Data Interoperability

The system aims to allow high degree of information flow between agencies. The primary challenge is information interoperability. This is especially so when attempting to link systems across different agencies and vintages. The system should allow retrieval, query, correlation and fusion of data across different data sources, operating on different platforms and query methods. Besides the data connectivity, the meaning and context of information must be preserved with minimal uncertainty.

Content managers will establish the linkages between information sources based on the operational needs. With the help of middleware, content managers will establish the data conversion matrix between data source. Based on the matrix, the middleware will support the exchange and manipulations of information from different sources and format. In this way, ad hoc and rapid inter-connecting of data sources can be achieved and a coherent situation picture can be presented to users or applications.

An intelligence data broker layer will facilitate the translation of information while preserving the meaning and context. Using translation rules, a data broker layer will support the integration of the data sources at the same time, preserving the meaning of information when it is being accessed by another agency. If there are to be losses in accuracy or uncertainty as a result of the translation, these need to be explained so that decisions can be made with these taken into consideration.

For information which cannot be translated automatically via data broker, content managers will perform manual conversion/translation. He will be provided with the necessary tools to perform these tasks efficiently.

b. Support for Ad Hoc Structure

One of the key success factors in Singapore's SARS incident was the ability to form ad hoc organizational structure and implement processes which span agencies. One of the primary focuses of the proposed system is to enhance the effectiveness of collaboration and the ability to execute ad hoc processes which are created as a result of the collaborations. The formation of ad hoc structure entails bringing people from different domains of expertise together. The most effective form of collaboration is still to have face-face meeting where beside verbal communication, non-verbal communication such as gestures and cues enhances the collaboration process. Technologies may be employed if such face-to-face meetings are not possible. However, technology can also be employed to enhance the effectiveness of individuals collaborating. Individuals can be provided with higher quality information, background information of others in the collaborations to better understand each other's point of view, tools to query rich source of information during the collaboration process.

The outcomes of such collaborations are actions plans or new processes. Humans, being habitual, are prone to mistakes when new processes are being introduced. The proposal system can enhance the execution of new processes with automated inter-agency processes to complement the manual processes.

c. Support for Mobility

In dealing with unconventional situation, ground executors need to be mobile so as to react to situation on the ground. They should also be provided enhance information services which can improve their effectiveness. Information services such as mapping service, 2nd level information services, role-based information service, and location based information service.

F. THESIS OUTLINE

The thesis takes a retrospective study of the SARS incident in Singapore. It identifies critical factors in Singapore fight to contain the SARS outbreak and propose a technical to support network centric operations in dealing with such unconventional crisis. The architecture amalgamates the various information technologies and demonstrates how the various sub-modules can work together to tackle unconventional crisis.

In Chapter II, NCW framework and concepts will be presented. Various armed forces have different definitions and views when it comes to NCW. Instead of presenting various concepts, we will base our thesis primarily on the NCW works of US Department of Defense (DoD), Office of Transformation.

In Chapter III, NCW framework, concepts and information technologies employed within the fight against SARS will be identified. The aim is to determine how these helped in the episode.

In Chapter IV, we will use this as the case study to identify information needs and flow required in unconventional crisis environment. In Chapter V, we will propose a technical architecture to maximize the leverage on information to effectively and efficiently combat asymmetric biological threats such as SARS.

We will conclude the thesis with recommendations and possible areas for further studies or research.

II. NETWORK CENTRIC WARFARE

A. IMPETUS FOR NETWORK CENTRIC WARFARE

There are different views and definitions as to what network centric warfare is. Despite these differences, there is a common underlying essence. Information and how organizations uses information is the underlying belief that NCW will fundamentally change the way military operates. It is the military version of e-commence. The main differences are the interpretations of what are the organizational behavior and changes, and how information is to be *exploited*. Debates are on issues such as: Should we revolve information around organizational goals and processes or revolve organization around information, and what *type* of information yields the maximum returns in terms of effectiveness or improvement in efficiency. To understand the essence of NCW, it is perhaps important to understand the background and impetus that lead to this impending revolution in military operations.

The impetus can be broadly classified into 2 areas although factors within each group will inevitably interlink with each other in a lesser way.

1. Emerging Challenges

a. Unpredictable Global Politics

The global politics is undergoing reconfiguration. At the global level, the international system is perplexed by the end of cold war, China's emergence as a global power competing for influence, expanding European Union, and Japan's fluttering economy and influence in the Asia region. At regional levels, countries are realigning with supranational organizations[3] and forming regional political and economical blocs. Such reconfiguration is

[3] Such as United Nations, World Trade Organizations

proceeding precariously, stabilized only by lack of powerful rouge state or player and increased trade interdependence of states.

b. Terrorist and Insurgence Threats

While the threat of global or large scale, state vs state war has reduced, threats of conflicts at lower level have increased. Sep 11 2001 attack, Bali bombing and subsequent events throughout the world illustrate the new form of threats faced by the world. Terrorist and insurgence groups formed and emerged, and threaten to destabilize the international and way of life of others. As these groups are mostly non-formal political entities, they do not conform to established rules or norms. They employ asymmetric and unconventional tactics, mostly have low respect for humane warfare and do not observe established international rules of engagement.

These non-state actors are primarily driven by shared faith and beliefs. Through these faith and belief, they achieved a high level of self-formation and synchronization, and with reduced organizational burden and delectability. They blend themselves amongst people both in the physical and cyber space. Peacetime structuring, preparation and training to engage these elusive enemies are difficult.

2. Changing Environment

The other primary impetus is the changing environment. This environmental change is brought about as we move into the information age which is fundamentally driven by information technology. “emerging information technology are fundamentally reshaping the global environment in ways unthinkable in the past”. [John & David, 2004]. At the same time, the environment also fuels advances in information technology in return. The following key factors are within this interplay of environmental changes and information technology:

a. Advances in IT Capability

Computational power, storage capacity and speed of information transmission have seen phenomenal growth within the last few decades. Computational power has been conforming to Moore's Law by doubling every 18 months. Hard disk capacity has even outperformed Moore's prediction and memory management methods such as caching boost the overall performance of a memory system. Advances in chip manufacturing also increased the speed of communication and network devices.

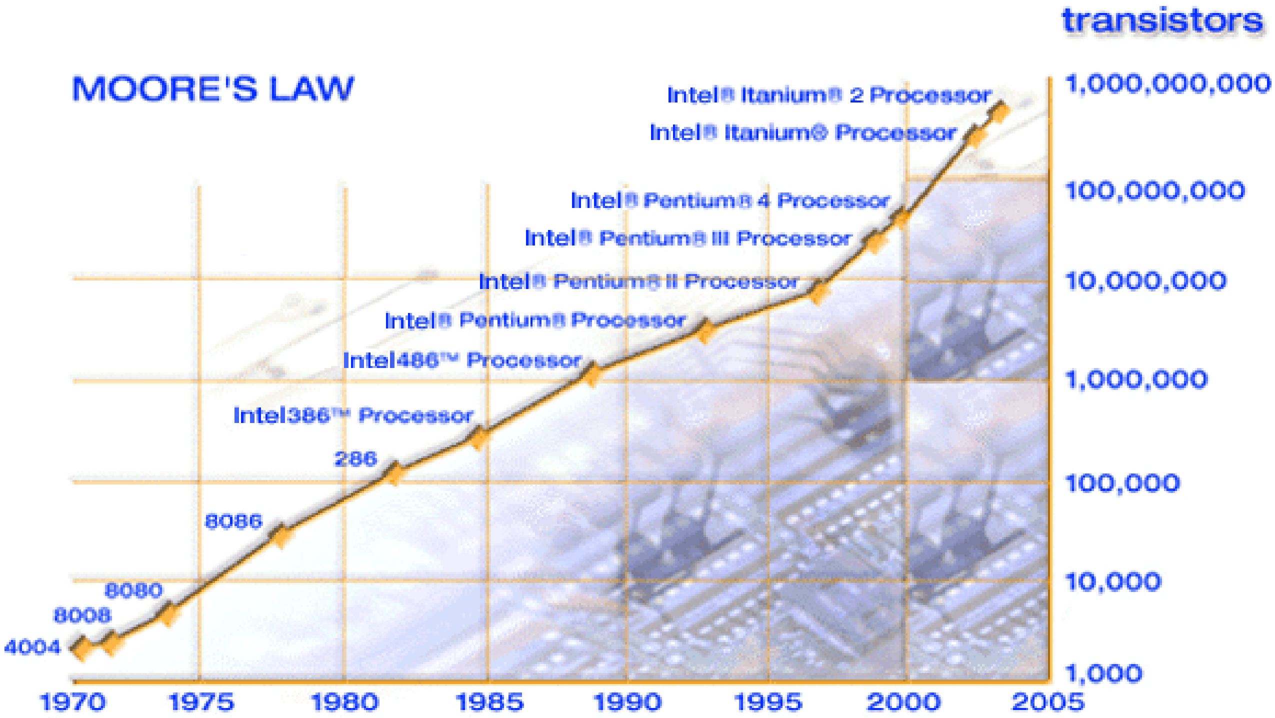

Figure 2. Moore's Law [www.intel.com/research/silicon/mooreslaw.htm, 2004]

Together with other technologies such as TCP/IP, web browser, point and click interface, ushered in the information age. All these resulted in dramatic increase in our ability to capture, manipulate and handle information.

b. Connectivity, Portability and Mobility

Not only are we able to handle more information faster, the Internet, media coverage, mobile devices and services also increased our connectivity to people and information sources. Using Metcalfe's law, the "utility" or "value" of network increases proportionally to the square of the number of nodes:

$$Value \propto (Number\ of\ \ Nodes)^2$$

However, David Reed pointed out the value of networks is based not only its point-point connection ability, but its group-forming ability. Based on that, the value of network increases proportionally to 2 raised to the power of number of nodes:

$$Value \propto 2^{(Number\ of\ \ Nodes)}$$

[www.reed.com/Papers/GFN/readslaw.html - 9 Nov 2004]

These increased value and the ability to share information transcends international boundaries and governmental organization. This facilitated the formation of virtual communities, interest groups and supranational organizations and challenges traditional governance. They are also being exploited by groups or individuals to advance and promote their ideologies and values.

c. Globalization

Globalization is characterized by increased connectivity between societies due to telecommunication, Internet, transportation, information flow and trans-cultural exchanges. Globalization brings like-minded people together in various ways, increased international trade, cultural exchanges and increases cultural diversity.

On the other hand, globalization also increases the potential for clashes between beliefs, religion and cultures. Countries dependence on global trade also increases their exposure and risk to events in other parts of the world.

B. ARMED FORCES RESPONSE TO THE CHANGING ENVIRONMENT

Each nation has their perspectives as to how the changing global political landscape, raising threat and changing environment have on their countries. They are influenced strongly by regional factors and have prioritized the impact of these trends. Despite these differences, all share the common conclusion that the future is dynamic, filled with uncertainties and they face emerging threats of unconventional nature. In response, respective armed forces are reviewing their outlook and missions capabilities against the changing environment.

Most developed armed forces are embracing the concept of network centricity in their force structure and capability buildup. The belief is that network centricity will provide them the capability to adapt and evolve to meet new challenges, leverage on information and information technology to increase their combat effectiveness.

Though all agree that networks and information are common denominators, politics, existing organizational structure, budget and other factors influence respective armed forces' views of what network centricity means to them. Below are some definitions and expressions of what NCW means to some of the leading Armed forces.

> The ability to gather knowledge; to share it in a common and comprehensible form with our partners; to assess and refine it to turn into knowledge; to pass it to the people who need it in an edited, focused form; and to do it in a timescale necessary to enable relevant decisions to be made in the most economic and efficient manner
>
> UK DCDS (EC) 8 Nov 01 on Network Enabled Capabilities

> Network-centricity will help us to link national, ADF and coalition sensor, engagement systems and decision-makers into an effective and responsive whole. At its core, NCW seeks to provide the future force with the ability to generate tempo, precision and combat power through shared situational awareness, clear procedures, and the information connectivity needed to synchronise our actions to meet the commanders' intent. NCW will require an approach that integrates our existing processes and systems with new technology and doctrine in the most effective and efficient way.
>
> Senator Hon Robert Hill, Australian Minister for Defence
>
> address to ADF NCW conference May 2003

> Network Based Defence, NBD, is the concept for developing a new kind of defence through transforming today's force structure into a defence based on flexible, rapid and controlled engagement capabilities. Networking the commanders and warfighters enables smarter use of resources at the right time and in the right place. NBD also means a capability to adapt continuously to changing threats, new tasks and advances in technology
>
> Swedish Armed Forces

C. TENETS OF NETWORK CENTRIC WARFARE

For the purpose of this thesis, we will examine the US concept of network centric operations proposed in *Network Centric Warfare* [Alberts, Garstka & Stein 1998]. This publication describes NCW is as follows:

> NCW is about human and organizational behavior. NCW is based on adopting a new way of thinking – network-centric thinking – and applying it to military operations. NCW focuses on the combat power that can be generated from the effective linking or network of the warfighting enterprise. It is characterized by the ability of geographically dispersed forces (consisting of entities) to create a high level of shared battlespace awareness that can be exploited via self-synchronization and other network-centric operations to achieve commanders intent.

In DoD’s Network Centric Warfare report to Congress in 2001, 4 tenets of NCW are as follows:

1. Networked force improves information sharing.
2. Information sharing enhances the quality of information and shared situational awareness.
3. Shared situational awareness enables collaboration and self synchronization and enhances sustainability and speed of command.
4. These in turn, dramatically increase mission effectiveness.

The primary aim of these tenets is to increase the richness and power of information, which translates into military capabilities. Information need not flow in hierarchical fashion, instead it can be pulled from sources, push to relevant uses where it can increase the combat effectiveness.

> If you want to increase the richness of your information you get that by sharing it. The power of information comes in its ability to share it as opposed to the ability to hoard it.
>
> [Cebrowski, 22 Jan 2003].

With these increases, forces achieve enhanced shared situation awareness and self-synchronization amongst forces is faster. This reduces the Observe, Orient, Decide and Act (OODA) [Cebrowski 1998] step between applications of forces and increases the “speed of command” and disrupting enemy’s OODA loop.

In line with these tenets, there is a basic need to network forces together. Besides networking forces together, information must be made assessable, interoperable and understandable by users. These will achieve shared situational awareness. This shared awareness can then be translated to physical, actionable events.

D. DOMAINS OF NCW

In *Network Centric Operations Conceptual Framework V2.0*, John and David highlighted that changes must occur in the *Physical, Information, Cognitive* and *Social* domain before transformation in US DoD can happen.

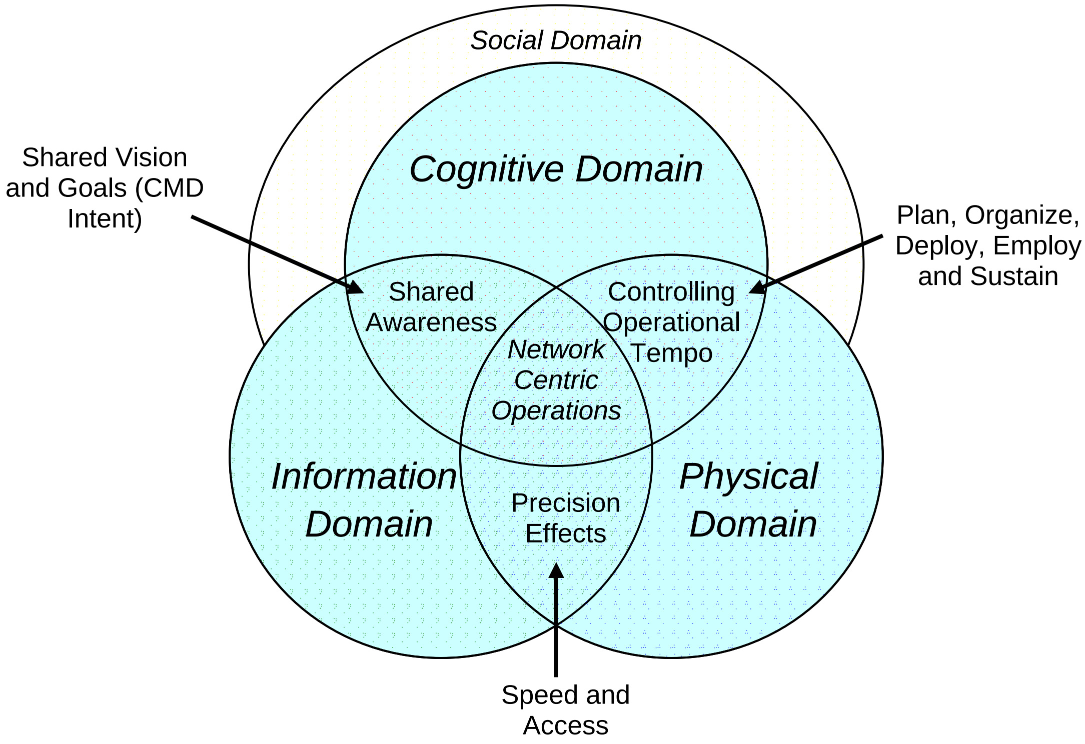
Social Domain
Cognitive Domain
Shared Vision and Goals (CMD Intent)
Plan, Organize, Deploy, Employ and Sustain
Shared Awareness
Controlling Operational Tempo
Network Centric Operations
Information Domain
Physical Domain
Precision Effects
Speed and Access

Figure 3. NCO Domain [John & Albert, Jun 2004]

1. Cognitive Domain and Social Domain

The cognitive domain is the domain where people become aware of their situation, understand what is happening, make decisions and take effective action. However, enabling individuals with enhanced awareness is necessary but insufficient to achieve the network centric effects. Entities participating within an operation must collaborate and achieved shared awareness through the activities which [Albert &John Jun 2004] termed as *shared sense-making*. The social interaction of the collaboration process plays a key role in achieving shared sense-making. Social interactions involve the cultural aspect of individuals, the team individuals are participating in and the larger context the team is operating within.

2. Physical Domain and Information Domain

Within the physical domain, strike, protect, deploy, and sustain operations takes place. The physical domain spans the traditional dimension of warfare in land, air, sea and space. It is within the physical domain where actions carried out and physical effects felt. In the traditional sense, force-on-force comparisons are made in this domain. To support NCW, network, communication and C2 infrastructure are established within the physical domain. It is within this domain that physical connectivity between nodes and network-ready nodes exist.

Within the information domain, information is collected, disseminated and value added. It is within this domain that situation awareness is shared though physical media, commander's conveyed and the combat power of the traditional forces is enhanced through exploitation of information.

Within this domain, the operatives also include contention for information. The fight is not conducted though the use of tanks, ships or planes, instead, it is conducted though the protection of information, speedy dissemination of information, disruption of enemy's sources of information.

It is within and between the physical and information domain where information are captured, disseminated and translated to physical effects, both domain need to be discussed as an integral whole. In [John & Albert, 2004], key capabilities necessary within these domains are:

1. Mobility. Mobility is the ability to command and control on the move. Entities are connected via networking infrastructure which allows them to have operational flexibility to access information from they are. Without the need for a fixed network infrastructure, it allows rapid deployment of forces, with reduced need for network planning and supports flexible organizational structures.

2. Interoperability. Interoperability is defined as

> the ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them/or their users. The degree of interoperability should be defined when referring to specific cases.

http://www.dtic.mil/doctrine/jel/DODdict/data/i/02749.html Accessed Nov 10 2004

US DoD focused interoperability on the physical connectivity whereas NATA focused on the information sharing. NATO specifies the following levels of information sharing

a. No data exchanges

b. Unstructured data exchange

c. Seamless sharing of data and

d. Seamless sharing of information

3. Security. Involves the protection of the integrity and functionality of the network and system systems, protection of information. It spans the physical domain of network and infrastructure and the management of information and requires the support of policy, training and processes.

III. NETWORK CENTRICITY IN SINGAPORE'S FIGHT AGAINST SARS

A. SARS INCIDENT IN SINGAPORE

1. Early Stage of the Outbreak

After the initial detection SARS virus in Singapore, the health professionals determined that standard infectious control measures would be sufficient to contain the outbreak. However, as little was known about this new virus, there were no standard treatments. Clinical judgment was required to determine if a person had been infected with SARS; medical professionals were unsure of the effectiveness of the isolation measures as the modes of transmission of the virus were not known[4]; in some cases, the virus led to complications in the patients while in others, the virus is masked by symptoms of common illness and went undetected[5]. With these uncertainties, standard contingency plans were not effective.

Media reports of the unknown and deadly nature of the virus seeded fear amongst the public. People felt unsafe to conduct their normal daily routine for fear of contracting the disease. High risk area such as public transport, hospitals, clinics, crowded places and high risk people such health care workers were avoided. The diagram below shows the early stage of the outbreak:

[4] WHO in March 03 - "But WHO does not know what is the right thing to do to control this disease nor would anyone else know."

[5] A 60 year-old man who suffered chronic kidney disease and diabetes had low grade fever and his chest X-ray were normal. Nothing indicated that he might be infected with SARS. He was treated in an open ward of a hospital and sparked an outbreak - infecting 62 people.

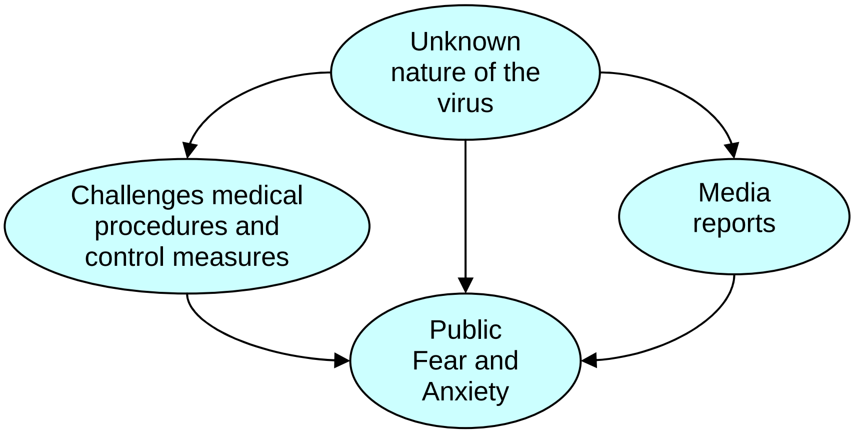
Unknown nature of the virus
Challenges medical procedures and control measures
Media reports
Public Fear and Anxiety

Figure 4. Early Stage of the Outbreak

It must be emphasized that the fear psychology of the society was so strong that it almost paralyzed Singapore. It is also arguable that it is the fear factor which eventually garnered the government's and people's resolve to contain the spread of the virus. The social psychology shaped the way Singapore Government and its people reacted to the episode.

> The unspoken fear on the streets can be infectious. Even I – with my c'est la vie attitude about car accidents, deadly diseases and premature ends – entertain wild thoughts every now and then. I look suspiciously at the chopsticks on my bowl of yong tau foo[6]. I wonder if the escalator banister has traces of someone's snot. In my most imaginative moments, I imagine deadly invisible missiles of saliva shooting out of people's mouth as they yak in a coffee shop. I wish I never learnt what 'exponential' means. Now, I find myself lying in bed working out the mathematical implication of a contagious disease and the kind of time frame before we all bite the dust.
>
> Columnist Kelvin Tong April 2004

[6] A favorite local dish in Singapore

2. Deterioration of the Situation

Within a short span of two weeks, the situation in Singapore deteriorated rapidly. Several factors interplayed and provided negative feedback to each other. This resulted in the situation spiraling out of control. The primary cause of was the fear and anxiety of the public. Due to the interplay and interdependence of factors, the situation is unpredictable. An action or in-action that changes the current condition may lead to drastic deviation in the eventual outcome. The situation has the characteristics of a non-linear, complex system.

A non-linear, complex system is one in which a small difference in the initial conditions will result in a large variation in the eventual state of system.

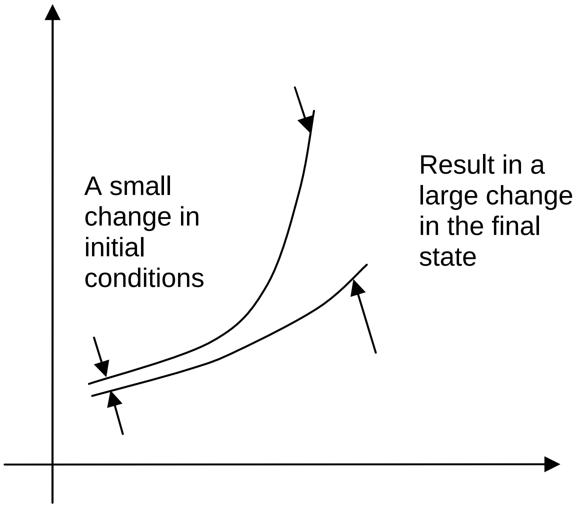
A small change in initial conditions
Result in a large change in the final state

Figure 5. Non Linear, Complex System

As an example, a Singapore man was infected when he came in contact with an SARS index case. Contact tracing of the index case failed to identify the male and he was not quarantined. Subsequently, he fallen ill and visited two separate hospitals. Both hospitals did not diagnose him as a SARS patient. He sparked off an outbreak outside the hospital cordon into the community at large. The outbreak happened in Singapore's primary fresh produce distribution centre – Pasir Panjang Wholesale Center.

The outbreak disrupted 70% of fresh supplies to Singapore, affected the livelihood of thousands of stallholders and workers, posed high risk to evolve into a nation wide epidemic due to high human traffic and the connectivity these people have when they branch out to retail outlets and buyers.

Besides all these factors, the Singapore Government was also fearful of outbreaks in key areas that may threaten the functioning of critical infrastructure in Singapore. The various factors and looming fear intertwined and convoluted the entire situation.

3. Intertwined Scale-Free Network of Problems

To appreciate the intertwined nature of the situation, various factors and their effects on each other are mapped out. Figure 4 probably resembles the interplay of the factors and the worries Singapore Government had during the height of the SARS outbreak.

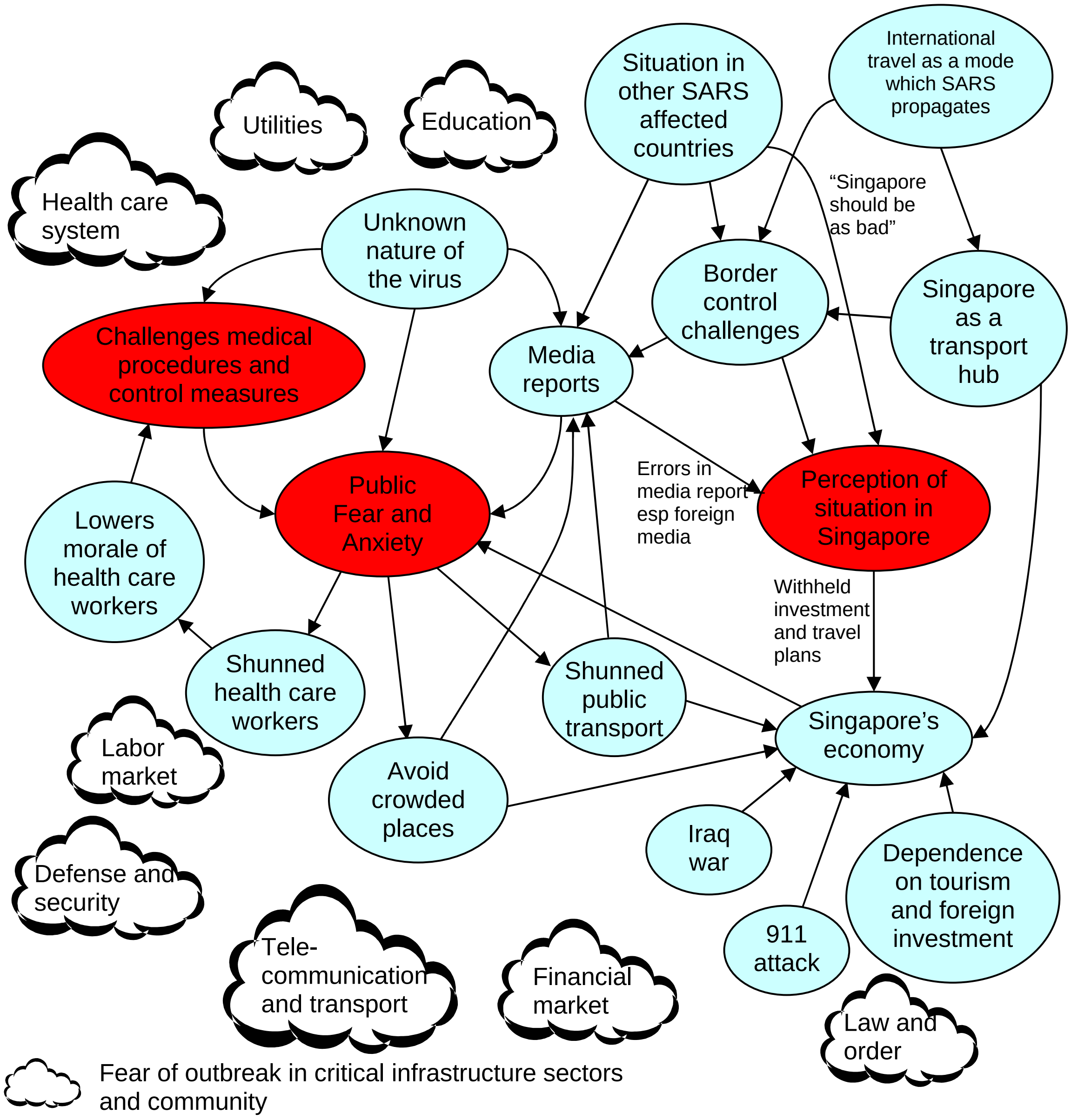
Utilities
Education
Health care system
Situation in other SARS affected countries
International travel as a mode which SARS propagates
Unknown nature of the virus
"Singapore should be as bad"
Border control challenges
Singapore as a transport hub
Challenges medical procedures and control measures
Media reports
Public Fear and Anxiety
Errors in media report esp foreign media
Perception of situation in Singapore
Lowers morale of health care workers
Withheld investment and travel plans
Shunned health care workers
Shunned public transport
Singapore's economy
Labor market
Avoid crowded places
Iraq war
Defense and security
911 attack
Dependence on tourism and foreign investment
Tele-communication and transport
Financial market
Law and order
Fear of outbreak in critical infrastructure sectors and community

Figure 6. Intertwined Network of Problems

Having determined the network of issues and their interaction, the Singapore government quickly determined that the center of the situation is the fear and anxiety of the public. Along with it, several other factors such as international perception of situation in Singapore and the medical challenges were also critical in keeping the situation under control. These are the hubs in a "scale-free" network. Tackling these hubs will bring about the rapid collapse of this network of problems [Barabasi 2002].

B. SOCIAL AND COGNITIVE DOMAIN OF THE SARS BATTLE

1. Recognizing That There Will be a Problem

The initial challenge in the battle is recognizing that there is a problem and the scope of its impact. By linking pieces of information, staffs at the MOH determined that there is an outbreak at hand[7]. However, they assessed that the problem is containable within the medical professionals. On Mar 18, 2003, Minster for Health Mr Lim Hng Kiang reported to Singapore Parliament that there was no cause for alarm and was confident of the infection control measures. The belief then was that SARS is transmitted by close contact. However, lack of information about SARS, the public fear and anxiety it caused, media reports and Singapore positional as a key international transport hub forces resulted in the spillage of effects to other sectors of Singapore.

It was only a few weeks after the detection of the first SARS patient in Singapore before the Singapore government determined that the situation is beyond medical domain and required other agencies to come in[8].

The challenge is how does one visualize the situation and determines that there is a potential problem based on information from multiple, seemingly unrelated sources. From a complex, inter-reacting and dynamic situation, determine the underlying relationship and order, and predict or anticipate the future projectile of situation.

[7] On March 6, a TTSH doctor alerted Ministry of Health (MOH) Singapore about three patients with pneumonia-like diseases who are not responding to standard treatment. Together with information that a medical evacuation team had been involved in transport a patient with a mysterious disease from Hanoi to Hong Kong and rumors of a mysterious pneumonia outbreak in southern China coalesced at MOH Singapore and allowed the ministry to piece together the possible scenario that they had a new disease outbreak at hand. [Chua Mui Hoong 2004]

[8] "Until April, SARS was primarily a problem residing with the Ministry of Health (MOH). For much of March, the SARS battle was lef by Health Minister Lim Hng Kiang, PS MOH and its director of medical services Dr Tan Chorh Chuan." [Chua Mui Hoong 2004 Pg 119].

2. Collaborative Group Decision Making and Consensus Building

Having an individual or a small group determined that there is a potential problem is insufficient. This perceived problem must be conveyed and be shared by majority of the larger community concerned before effective actions can be taken. Depending on social context, dynamics, individuals and the situation at hand, this 'tipping point' varies. In some cases, a problem was identified, however due to circumstances; influences of various other factors and social dynamics, no actions were made to rectify the situation. Breaching the tipping point usually requires the build-up of multiple, seemingly small events, culminating in the breach.

By mid March, Ministry of Health recognized that it requires efforts from other agencies. It enlisted the help from other agencies such as nurses from Health Promotion Board, Singapore; People's Association, Singapore and Cisco in serving home quarantine orders; Civil Aviation Authority of Singapore and Ministry of Transport to screen travelers at border points.

However, this recognition within Ministry of Health is not sufficient to breach the tipping point. The early efforts were primarily from a single ministry – Ministry of Health.

Feedback from concerned parents about the safety of sending their children to school, a powwow session between Deputy Prime Minister, Minster for Health and Minister for Education, and subsequently the decision to close schools for several weeks set the environment for group recognition that SARS is more than just a medical problem.

A weekly Cabinet meeting held during April 03 provides the final tipping point. As a result of the Cabinet meeting, decision was made on Apr 03 2004 to convene the Executive Group to deal with the SARS problem.

3. Scoping the Problem and Determining the Solution

Another key aspect in dealing with unconventional crisis is the scoping of the problem and the determination of solution. Recognizing that there is a serious situation at hand, the Singapore Government determined that the situation is a web of interlocking issues. Tackling each issue by itself yields limited effects. Tackling several issues at the same time, synchronizing and providing positive feedbacks to others issues will maximize the overall effectiveness. However, to effectively execute and synchronize actions across different agencies required changes in the inter-agency processes.

The Singapore Government also recognized that fear and public confidence is the heart of the situation. Several task groups were formed tackling different aspects of the situation; however, the underlying aim for each task group was to restore public confidence and allay fear of the situation.

C. INFORMATION AND PHYSICAL DOMAIN OF THE SARS BATTLE

1. Changes in Organization and Processes

Once it was recognized that fight is more than beyond medical problem and resources from agencies other the Ministry of Health were required, it was also recognized that the existing governmental organizational structure was unable to effectively deal with the situation. The existing structure is effective and efficiency to deal with daily governance of the country but unable to deal the challenges of this unfamiliar situation.

The creation of the Inter-ministerial Committee, the Executive Group and the Inter-Ministry SARS Operations Committee were perhaps the most important actions taken during the fight against SARS. The structure provided horizontal and vertical integration of the various agencies involved in the fight against SARS. It also provided increasing granularity of execution control. The overall structure is as shown below:

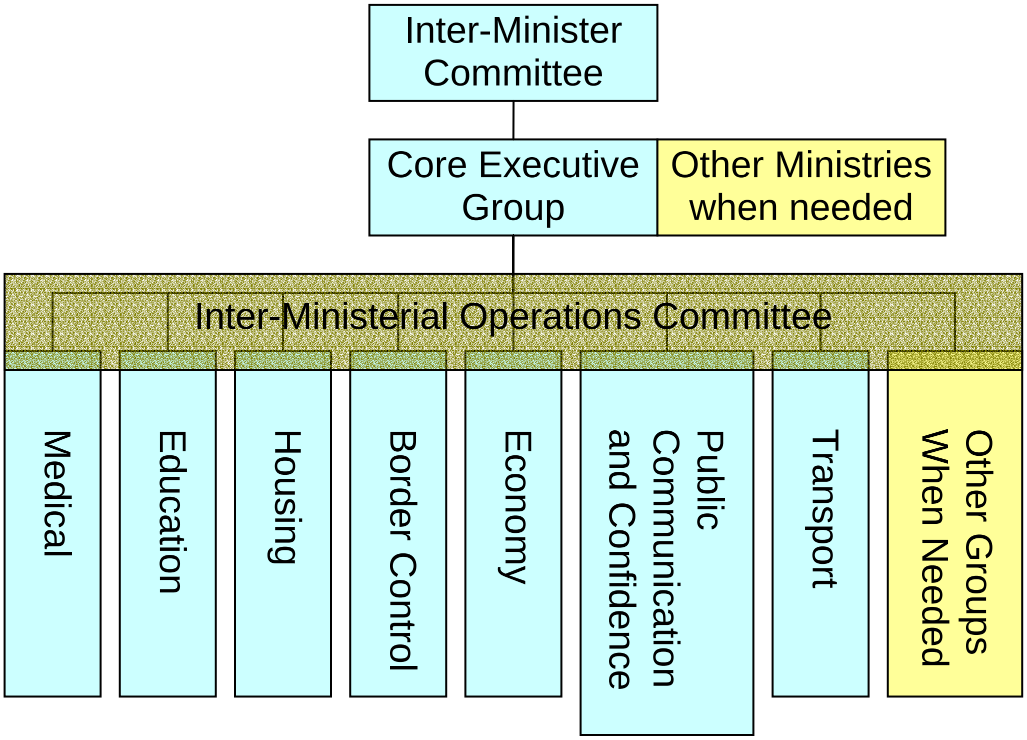

Figure 7. Organizational Structure for Fight Against SARS

The 9-member Inter-Ministerial Committee was the forum for making strategic decisions and approved major decisions and control measures. It provided guidance and oversight of the EG in the fight against SARS. The Inter-Ministerial Committee is chaired by Minister of Home Affairs and comprised 8 other ministers. The committee provided the horizontal integration across the ministries. It ensures that the views from various ministries were consulted. If necessary, decisions were further sanctioned by the Prime Minister or approved by Cabinet. These decisions were handled down to EG to be implemented.

The Core Executive Group (EG) was formed in early April comprising Permanent Secretary (PS) of Home Affairs, Health, Defense and Foreign Affairs. The EG is chaired by PS of Home Affairs. Other ministries were roped in whenever necessary. The EG was tasked to manage the crisis, coordinate and direct all necessary resources to contain and eliminate the SARS disease. The

EG develop plans, identified and allocated all necessary resources to implemented decisions made by the Inter-Ministerial Committee.

To manage the efforts in finer resolutions, two sets of working committees were form: the Inter-Ministerial Operations Committee and focused subgroups.

Sub working groups were formed to look into specific areas. For example, one sub group was tasked to tackle all SARS related housing needs. The primary task was to provide emergency quarantine housing and working out contingency plans for en masse decanting of residents. Other subgroups addressed transport, education, medical, border control, public communication and economic issues.

These working groups rallied resources, which may be from other agencies, necessary to achieve their mission objectives. As an example, the housing subgroup was responsible to provide housing needs such as emergency quarantine housing. The subgroup enlisted the help of Tourist Promotion Board to get hoteliers in Singapore to provide guest rooms for people required to be quarantined; People Association to work out food distribution.

The Inter-Ministerial Operations Committee on the other hand was established to strengthen inter agency coordination and operations. The actions and activities of the subgroups were coordinated and synchronized through the Inter-Ministerial Operations Committee.

Besides providing the necessary inter-agency integration, the organizational arrangement was also flexible enough to adapt to changing needs. Ministries and agencies may be roped in whenever it is deemed that their expertise or resources were required.

2. Collaboration, Decision Making Process and Share Vision

Having an organization that facilitated inter-agency integration and adaptable to situational needs alone is insufficient. When different agencies came together, they each had their own perspective of the problem and constraints. Normal team building processes would take weeks if not months. However, in Singapore's context and specifically the SARS incident, the process was much faster. The likely reason for this could be the all involved felt the gravity of the situation. Through daily updates, the Singapore government impressed upon the people and the civil sector the severity of the situation.

The daily updates and media reports also functioned as an effective communication between the government and people. Through honest and direct communication and updates to the public, the Singapore government was able to dispel fear and win the support and trust from of the people.

The shared vision amongst the agencies and between the government and people hasten the decision making process, achieved synchronization and facilitated execution.

3. Multi Agencies Processes and Executions

With a shared visions and flexible organization, the Singapore government was able to plan and execute multi-agencies processes. As an example, to restore consumer confidences and tourist, PM Goh directed for a "SARS-free corridor" be established. The concept of the SARS-free corridor was simple – to ensure that the airports, seaports, hotels and tourist places were all SARS-free so that tourist can feel safe to visit Singapore.

However, the execution is far from simple. A task force was formed under Singapore's Ministry of Trade and Industry (MTI). To create the sanitized corridor, Singapore's MTI enlisted the help of Singapore's Tourist Promotion Board (TPB). Together, the two agencies worked out the "Cool Singapore" Program. Under the program, an eight-point criterion[9] was established for hotels and retail establishment to follow. Certification teams would audit these establishments every two weeks. Within two weeks, 180 shopping malls had

[9] Appoint a SARS manager, conduct daily temperature checks on all their staffs, suppliers and vendors, disinfect premises daily and ensure staffs do not visit SARS-affected countries over the past 10 days.

been certified. 89 hotels, three limousine services, Changi Airport, The Esplanade[10] and the Singapore Expo convention centre also participated in the program.

To correct the perception tourist had about the situation in Singapore, a website was established, live webcams showing that people going about doing their daily chores in shopping malls were also provided. An accompanying "Step Out Singapore" program was also launched together with the retailers. The S$2 million promotion effort lured back shoppers and tourists. It was estimated that the promotion effort generated over S$180million in turnover. More importantly, it drew people back onto the streets and shops again. At the community level, Singapore's National Environment Agency (NEA) launched the "Singapore's OK" program to promote hygiene. The Citizen's Consultative Committee also worked with the NEA to spread the message to coffee shops, markets and other outlets.

To correct the international perception of the situation in Singapore, a multi-agency, International Image task force was established. The primary aim of the task force was to project Singapore's international image during the crisis. The task force was head by Singapore's Ministry of Information, Communication and Trade. The task force included Singapore's Ministry of Foreign Affairs which monitored media reports and sought to verify with hospitals or individuals. Other agencies included Contact Singapore, Ministry of Manpower, Singapore Tourist Promotion board, Economic Development, Civil Aviation Authority of Singapore, Ministry of Trade and Industry and International Enterprise Singapore. The task force verified the reports in various foreign media and alleged exportation of SARS cases to overseas. It then worked through the various agencies and rectified the reports.

4. Information Sharing

To support the execution of the plans, information was shared freely between agencies. For example, to prevent the exportation of SARS patients out

[10] Theatres on the Bay arts center.

of Singapore to other countries, the Immigrant Control received updated list of people served with home quarantine orders. They could check and deny exit if anyone who was on home quarantine orders and attempted to leave the country.

To effectively contain the spread of virus, a system of contact tracing was also established. Whenever a patient is diagnosed with SARS, the contact tracing center in Ministry of Health will attempt to identify who might had came into contact with the patient. These people were classified as 'contacts' and will be issued home quarantine.

During the early stage, the contact tracing was carried out by a team of about 60 officials from Ministry of Health. The contacts of a SARS patient range from his family members, his colleagues at his working place to staffs and other patients in hospital or clinics during the time he visited. Pieces of information from various ministries and agencies were used to trace the contacts. Information from National Registration Office gives details of the patients of his family members; Ministry of Manpower provides information about his employment and information from hospitals provided details about patients and staffs that might be within the vicinity of the SARS patient concerned. In the later stage, linking up the various databases improves the overall efficiency further.

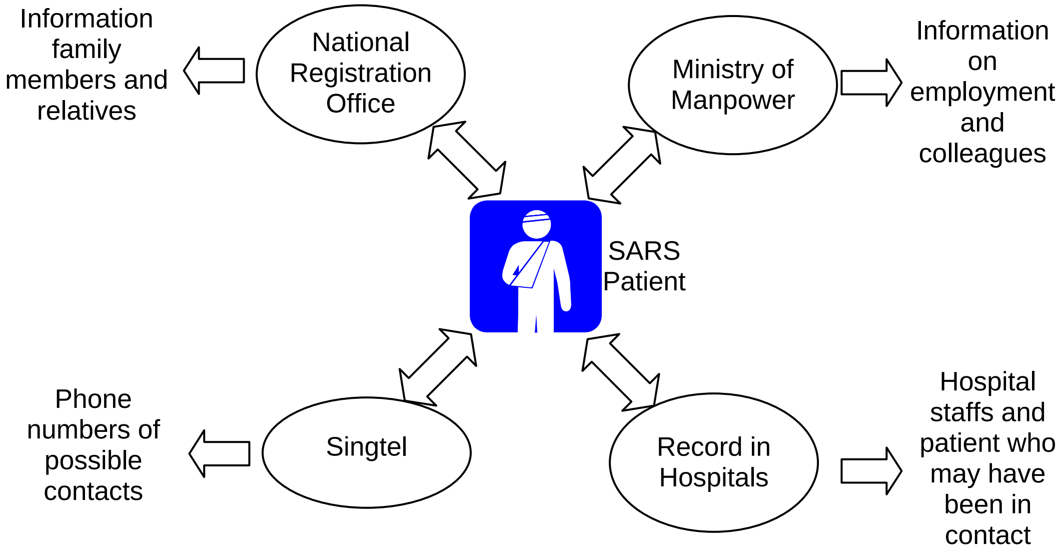
Information family members and relatives
National Registration Office
Ministry of Manpower
Information on employment and colleagues
SARS Patient
Phone numbers of possible contacts
Singtel
Record in Hospitals
Hospital staffs and patient who may have been in contact

Figure 8. Information for Contact Tracing

5. Employment of Technology

When SARS virus break out in Pasir Panjang Wholesale Center, some 2,400 people needs to be contacted and determined if they needed to be served home quarantine orders. The manual contact tracing systems showed its limitations. The manual systems used spreadsheets and manual record keeping which was slow and inaccurate. People were served with late quarantine orders or were served twice.

The Defense Science and Technology Agency (DSTA) was roped to provide assistance in deploying technological solutions in the fight against SARS. Working with IT departments of various ministries, Singtel and Ministry of Information, Communications and the Arts (MITA), linkages between databases of several key institutions and agencies were established. This increased the overall efficiency and effectiveness of contact tracing.

To track the movement of staffs, patients and visitors to hospital, Radio Frequency ID (RFID) systems were deployed in hospitals. RFIDs tags worn on waist tracked the movement of people, and logged down the time and place within the hospital a person had been to. In the event when any person within the hospital was diagnosed with SARS, the database allowed the tracing of where he had been to in the hospital, at what time and who were around him at those points in time.

D. THE GLOBAL BATTLE

While Singapore established networks of people and procedures in the fight against SARS, it also participated in the larger global battle. Singapore prevented exporting of SARS to other countries through its contact tracing system and tight border controls. At its border checkpoints, Singapore established thermal scanners to seek out travelers who exhibited feverish condition. Being a key traveler’s hub, this helped reduced the transportation of potential SARS patients between countries.

Singapore also participated in the global network of medical research to find solution to the deadly virus. It was part of a network of 11 laboratories from around the world. After several weeks, Genome Institute of Singapore (GIS) was the third to publish its SARS sequences and eventually presented the most number of genome sequences. With a large pool of sequences and through sharing with other institutes around the world, GIS also determined that the virus has a mutation rate of 0.03 per cent per generation. Singapore also participated in the WHO Global Outbreak and Alert network.

E. LESSONS LEARNT

From the SARS episode, we learned that to deal with unconventional, evolving situation, there is a need to take a network-centric view of situation. One needs to identify issues involved and the interaction between these nodes. This will help in the formulation of the solution. However, one also needs to recognize the fluidity of the situation. Due to this, a multi-agency and flexible organization is essential. This allowed rapid adaptation to deal with the situation.

Ad hoc organization comprises people from diverse backgrounds and culture. To enhance the effectiveness of ad hoc teams, it is essential to rapidly identify and foster a common vision which all can agree and associate with.

Free flowing of information is also required to enable the execution of inter-agency processes. Technology can be deployed to further enhance the overall effectiveness and efficiency of newly created inter-agency processes. Human are flexible in adapting to situation but are prone to make mistakes when under stress, executing new routines. Technology can be deployed to assist the human and minimize such mistakes.

Technology can also be deployed to enhance the interoperability of organizations. Mobile solutions will provide ground enforcers the mobility and agility needed to deal with dynamic and changing situation on the ground.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. REQUIREMENT FOR NETWORK CENTRIC OPERATIONS

A. INTRODUCTION

In this section, we will discuss the requirements for a technical architecture that can support the use of network centric operations concepts to deal with unconventional crisis. This architecture can help to maximize the effectiveness of a multi-agency task force comprising of both fixed and mobile teams sharing the common objective of combating an asymmetric threat like a biological or disease outbreak in an urban and highly populated area. The Singapore SARS incidence will be used as a case study to substantiate the requirement, scope the problem into an appropriate context and validate the effectiveness of the architecture.

Due to the high degree of uncertainty and the need for large scale cross agency coordination, the tackling of asymmetric threats like the SARS virus presents unique challenges. Thus, having the ability to deal with the rapidly changing situation, anytime and anywhere, is paramount. Fundamentally the capability to communicate and collaborate while on the move would be a key enabler and a critical success factor.

B. BACKGROUND AND BROAD REQUIREMENTS

We will begin by discussing the broad requirements of the technical architecture. The following are the key focus for the technical architecture:

- To achieve the required level of shared situation awareness by improving information sharing and enabling seamless exchange of information between the different agencies, taking into considerations the heterogeneous setup.
- To enhance communication and collaboration between the multi-

agency task force involved in the combat of an asymmetric threat like the SARS outbreak.

- To maintain the responsiveness and the agility of the mobile teams.
- To help the users make accurate and timely decisions.

This architecture shall be developed in the context of Singapore, which is a small city state comprising of mostly densely populated areas. The information technology and communication infrastructure in Singapore is highly developed with broadband and cellular phone coverage close to 99%. With the fruition of the IT2000 vision that started in 1992, Singapore has transformed into an intelligent island where information technology is embedded in all aspects of the daily life for the Singapore citizen. [Yong]. Though the Civil Service Computerization Program (CSCP) that started in 1981 to computerized and interconnect all the ministries, statutory boards and government linked organizations, the entire government is now fully computerized with many government services accessible round the clock from the Internet. Thus, it may appear that the development of an architecture to facilitate multi-agency information sharing and collaboration is an easily achievable task. However, this may not be so as the entire CSCP took many years to complete using different generations of technologies involving mainframes, client-server systems and web-based systems. Also, most of the computerization programs started off with the core objective of enhancing internal workflow and efficiency. Asymmetric threats demanding rapid information sharing and collaboration across different agencies on an ad-hoc basis is a recent requirement. This is currently associated from the homeland security perspective. Most of the systems were not designed and constructed to fit into the kind of flexible environment required to enable ad-hoc interoperation between different agencies. Therefore, the challenge is to develop an architecture that will allow the heterogeneous system and technology from the different agencies to work seamlessly to tackle a complex and time-critical problem, like the SARS situation in Singapore.

1. Key Challenges Involved

The challenge in dealing with such an asymmetric threat can be characterized as follows:

Firstly, the task force has to deal with a situation where there is incomplete and inconsistent information. The information could be wrong or mutually conflicting. Next is the need to work on a compressed timeline where time critical decisions are made in real time using all available information at the point in time. Lastly, the situation could demand the need to make decisions that could potentially have significant outcomes at a time where the situation is still undergoing rapid changes and a complete and consistent picture of the situation is not yet available.

C. KEY CONSIDERATIONS

After understanding the context of the SARS problem, the key considerations of our proposed architecture are summarized below:

- There are multiple agencies involved, all with different processes and information requirements.
- There are heterogeneous computer and communication systems, with different Operating Systems, hardware and applications software.
- There are different data formats involved. Not all the information can be available for extraction. Some could be proprietary.
- There is no single working solution available that can bind all the different systems together.
- The current solutions developed for NCW are skewed towards the needs of the military and build on the assumptions of the military. The military have some unique characteristics like having a well-defined hierarchical command structure, a doctrine driven workflow, a set of clear and distinct procedures to deal with different problems together

with constant training and retraining. Thus, the military can have the option to approach new problems by evolving existing system of solutions. A paramilitary or non-military multi-agency setup does not have any of these characteristics and advantages to exploit.

- The proposed solution to interface and retrieve relevant information from the respective databases must not adversely impact the functionality and performance of the existing system.
- The recommended set of solutions in the architecture must tap on existing infrastructure and technology, comprising of software and tools that are easy to learn and use. It shall support ubiquitous deployment requiring little or no effort to setup and configure.

D. USERS OF THE SYSTEM

In order to develop a comprehensive set of solutions that will form the architecture to meet the needs of the various groups of users and stakeholders, we will first attempt to categorize the different roles that are involved in the combat of SARS or similar biological and disease outbreak.

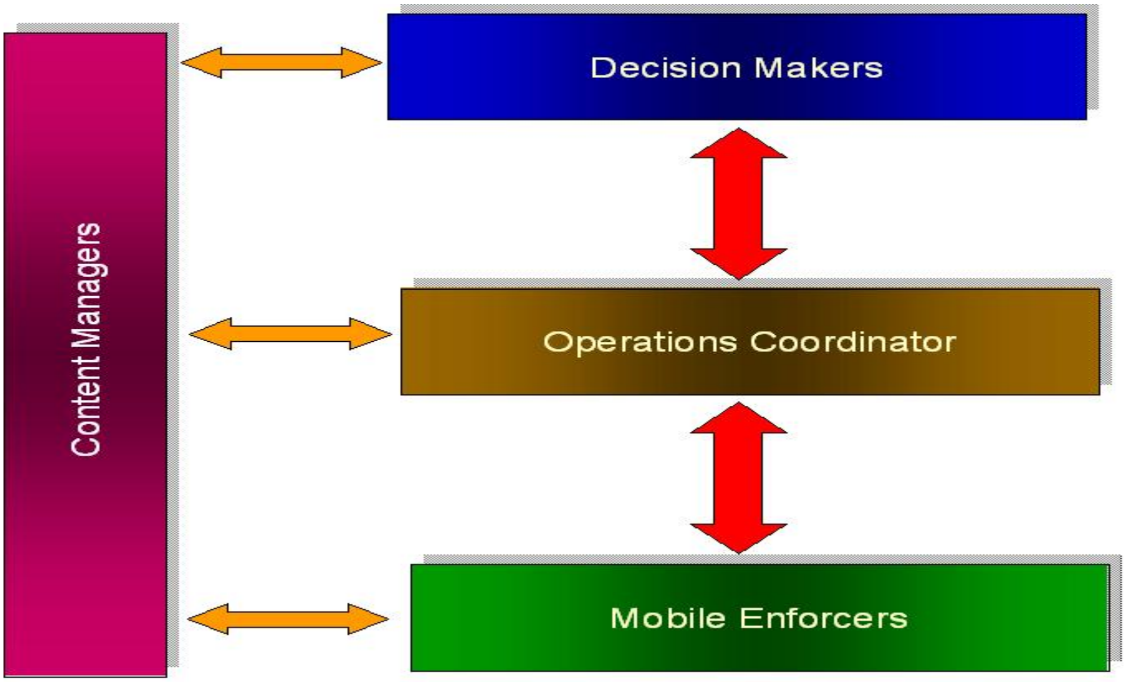

Figure 9. Four Different Classes of Users to be Supported.

As shown in Figure 9, there are four different classes of users that the system must support:

1. Decision Makers

The system must provide all the relevant executive level information and ensure that the decision makers attain the right level of situation awareness at all times to support their decision needs. A set of decision support tools shall be available to help manage alerts, monitor feedbacks, facilitate collaboration, provide context for the developing situation, disseminate orders and monitor the outcome of the decision. For this thesis, users in the SARS Executive Group fall into this category.

2. Operations Coordinators

This group of users will implement the decisions and the directions set by the decision makers. They are responsible for ensuring seamless inter-agency coordination by formulating the requirements for cross agency integration and process automation. They also work out the inter-agency processes and are responsible for orchestrating and calibrating the roles, responsibilities and workflow required for the ad-hoc teams to accomplish their mission.

3. Mobile Executers

They are mainly responsible for taking actions and enforcing decisions, which they can receive in real time while on the move. Mobile users also act as on-site human sensors providing real time ground information back to the operation headquarters. An example for such user is those responsible for serving quarantine orders for suspected SARS victim.

4. Content Managers

The Content Managers determine what information the decision makers and the various groups of users will need to perform their job. They have direct access to myriad sources of information and rely on software tools to discover, translate, reformat, filter and churn out the required type and level of information to support the respective group of users. The system shall provide a set of tools to work on the multiple formats of information that are drawn from the heterogeneous data sources, independent of Operating Systems, applications and hardware platform.

V. TECHNICAL ARCHITECTURE TO SUPPORT NETWORK CENTRIC OPERATIONS FOR UNCONVENTIONAL CRISIS

A. ARCHITECTURE FOR UNCONVENTIONAL CRISIS

After reviewing the objectives, requirements and key considerations, the proposed architecture that uses the network centric operations concept to combat unconventional crisis is depicted in Figure 10.

This architecture helps to ensure that a network of distributed organization components comprising of fixed and mobile elements can exchange information and coordinate activities in a flexible and scaleable manner. There are several key components to the architecture. The Unified Information Bus enables the seamless exchange of information between the various agency and software modules. A set of middleware solutions shall interface with the heterogeneous data sources which include the databases, file systems and data repositories. Through the set of middleware solutions, disparate sources of data shall be retrieved, filtered, reformatted, translated and collated into a collection of common data sources that can be formulated into an integrated, relevant and consistent situation picture. The Content Managers shall use a set of Meta-Data Management Tools and Data Processing Tools to perform unification of data dictionary and defining the data requirements needed for the mission. The Unified Information Bus enables the seamless exchange of information between the various agency and software modules. There is also a set of software modules and tools that can help enable the operation of the ad-hoc teams. Finally, the support for mobile computing shall be enabled by a set of Mobile Information Services that delivers timely and relevant information to the Mobile Enforcers, so that they can be responsive and precise in their action.

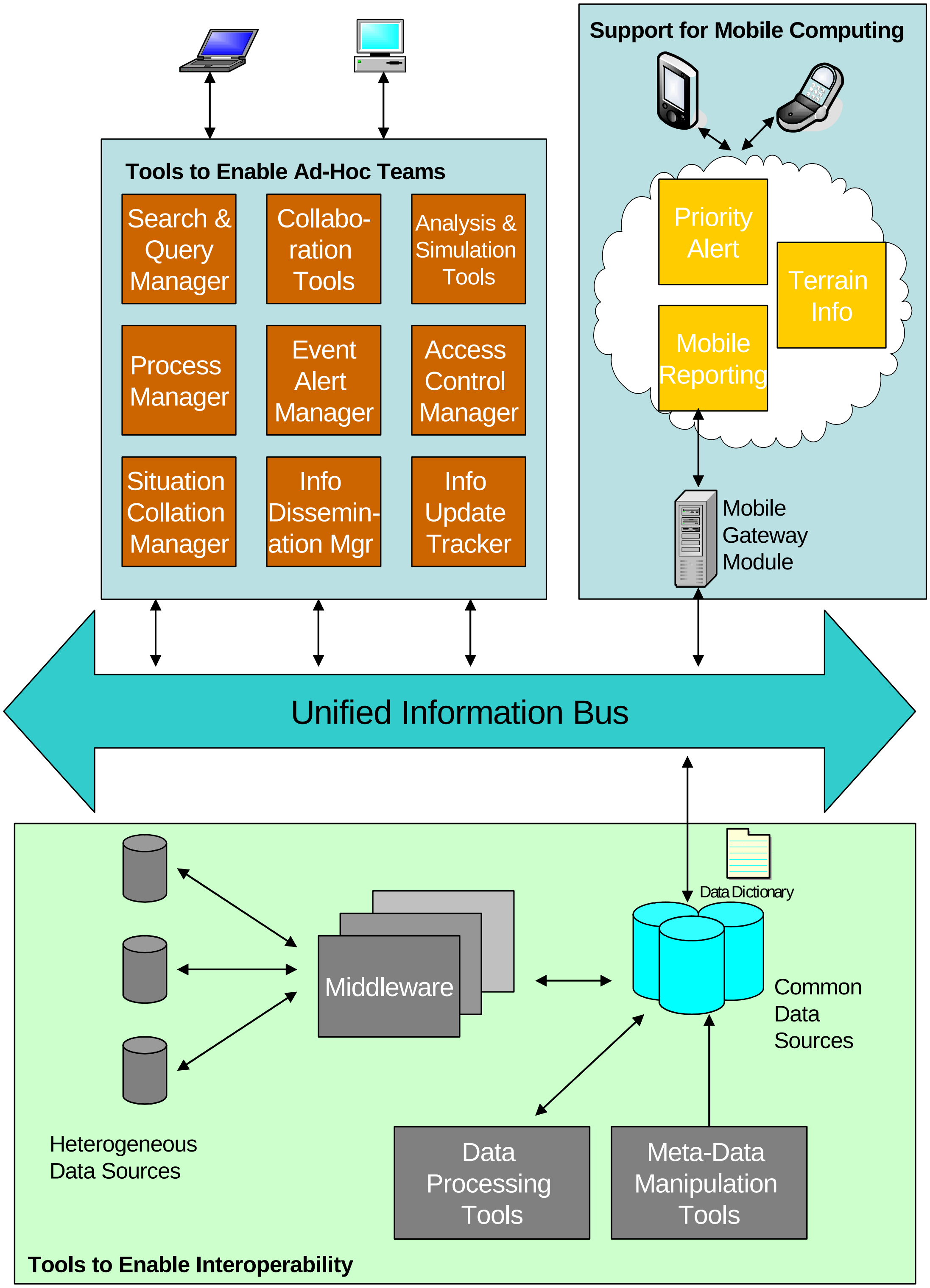

Figure 10. Technical Architecture For Unconventional Crisis.

B. UNIFIED INFORMATION BUS

The Unified Information Bus is the key enabler for shared situation awareness in the ad-hoc organization. Having situation awareness implies that one is aware and understands what is happening within a given environment at a given time. It is therefore crucial for users to be able to subscribe to information that is relevant for the mission. The Unified Information Bus can be implemented through the Message-Oriented middleware and critical information will be published as structured XML messages, facilitating loosely coupled asynchronous communication between applications.

C. DATA INTEROPERABILITY

To ensure the interoperability of an ad-hoc multi-agency task force, we must first ensure the interoperability of the people and the processes of the respective agencies. In order to realize this requirement, data interoperability is the key. Data interoperability allows the sharing and integration of data from the data sources of the different agencies regardless of hardware, operating systems, programming languages and databases. It involves the identification, retrieval, filtering, formatting, merging and translation of disparate data sources into a coherent information source that can be shared to raise the situation awareness of the ad-hoc teams.

While the derivation of a common data dictionary can facilitate effective sharing and exchange of information between the various agencies, it can be an extremely difficult, complex, costly and time consuming task. However, this is an essential pre-requisite to achieving data interoperability and this section will examine how it can be achieved.

The military have frequently talked about the need to have a common, relevant and sharable situation picture in the literatures for NCW. Analogously, in the fight against SARS, we need our Decision Makers, Operations Coordinator and Mobile Enforcers to get access to all the relevant information and attain the right level of situation awareness for the job. There is a need to collate the information from the data sources of the various agencies together with information from the open sources like the newspapers and the Internet.

The essential steps to achieve data interoperability are:

1. Identify the Information Requirement for the Mission

We begin by identifying the type of information required for a specific mission. An often heard notion is that due to a lack of precedence in dealing with some types of asymmetric threats, it is not possible to identify the complete set of information requirement. While this statement may be true, it is still essential to identify the best possible subset of the information needed so that a more efficient search and retrieval mechanism can be built. This is critical in ensuring that the right information can be located and accessed in a timely manner. To meet other information needs that can arise on an ad-hoc basis, a general text search engine similar to the facilities found in Internet searches, shall be provided.

An example of identifying mission specific information from the SARS episode can be seen in the case when there was a need to perform contact tracing of people in order to contain the spread of the SARS virus. Since this involved knowing exactly where a particular person lives, where he does his regular activities and his movement within and outside of the country together with the list of people who are in close contact with him, the information required will need to come from the data sources of a few agencies.

2. Identify the Data Sources to Fulfill the Requirement

In a multi-agency setup, each individual agency have their data dictionary and data sources like databases and file system closely integrated into their respective mission and work processes. Each agency can contribute to the information needs of the newly defined mission of the ad-hoc organization. The respective Content Managers will have to derive the details of the information requirement, deciding on the data fields and the format involved. The Content Managers will identify how the different data sources from the various agencies can be collated to fulfill the information requirement of the mission. If the data involved is expected to change over time, the rate and means of update will need to be addressed.

To better identify the data fields and format involved, the Content Manager for each agency will have to review their respective data dictionary. In cases where the data dictionary is not available or out-of-date, the Content Manager will have to define and update the data dictionary where necessary. The next step is to integrate and normalize the data dictionaries of the various agencies to derive a common operation database required for the mission. This data dictionary will contain meta-data information embedding domain specific knowledge about the data objects. The completed data dictionary will consist of all structured and unstructured information required for the newly defined mission and serve as a standard data definition and reference for the various agencies involved.

3. Identify the Information Needs for the Different Roles of a Mission

The different roles in a given mission will have their individual information needs. To maintain the appropriate context and to prevent information overload, the Content Managers will need to match the information needs associated with the role to the available sources of information. It would be useful to have a matrix that clearly depicts the role, the information needs and the interface involved.

For example, for the task force that is involved in contact tracing of SARS suspect, the Mobile Enforcer who is responsible for confirming the home address of the SARS suspect will only need the name, address and a photograph of the person. The Operations Coordinator for this particular mission who will decide on the extensiveness and the number of levels for the contact trace will need more elaborated information associated with a person’s movement, daily activities and the resources available to execute the contact tracing.

4. Retrieval of the Data Sources

After identifying the information requirements and how these requirements can be fulfilled, the Content Managers will need to examine the physical attributes of the various data sources. The operating systems, hardware platform, database packages, file types, file formats for each of the data sources will need to be examined so that appropriate solutions can be implemented to ensure that all the required information can be retrieved from the heterogeneous sources.

5. Processing of the Retrieved Data Sources

After acquiring the required data from the various sources, the data will need to be filtered to eliminate the unwanted attributes and values. Some of the data may require reformatting so that internal representation implemented for storage and communication efficiency can be processed and exchanged as meaningful text. After filtering and reformatting the data, the various sources can then be merged to form the common pool of collated information sources which can be subsequently integrated into a comprehensive situation picture. Further processing on the collated information sources are needed to ensure that applications that require a subset of the information or information of a different resolution can also make use of the collated information source.

D. TOOLS TO ENABLE DATA INTEROPERABILITY

There are several possible technical solutions that can help to enable data interoperability, all involving different levels of cost, effort, ease of scaling and complexities. The most expensive option is to take into account the multi-agency interoperability requirement and implement a new system to support it. The cheapest alternative would be to develop specific data wrappers for the data interfaces that were identified by the Content Managers, who must already have a good understanding of the data model and have an intimate knowledge of the type and format of the data required. As there is a need to preserve the functionality and investment of existing system, the most optimal approach is to leverage on commercial off-the-shelf middleware solution and use the set of data adapters and connectors provided to implement a common interface for retrieving the required information across the heterogeneous data sources. Furthermore, COTS middleware solution offers a host of other capabilities including transaction management, collaboration management, directory services, system resilience and security.

1. Meta-data Management Tools

These set of tools will help the Content Managers to derive a common data dictionary by allowing the users to easily sieve out the essential database, tables and fields independent of differences in hardware, Operating Systems and database software. It allows the Content Managers to work at the meta-data level and focus on the means to support the information requirement of the new mission, using the myriad of data sources from the different agencies.

The Schema Repository Manager provides a universal repository for the schemas of the various agencies, ensuring that the version control and access control to the data models are centrally managed. Thus, it provides the appropriate check-in and check-out mechanism at various granularities, centrally managing the operations up to table and file level. In this case, different Content Managers can concurrently work on the schemas that they are responsible for and the entire schema will be in-sync with each other.

The Data Modeling Tools allows the Content Managers to have a schematic view of all the databases and fields involved. It also provides a graphical interface that shields the Content Managers away from the complexities of the various Data Definition Languages associated with the different databases that they will need to work with. The tool will greatly assist the Content Manager in identifying, refining and normalizing the data from different applications into a common scheme that will form the unified data dictionary.

The XML Schema generator takes the consolidated data models and use the meta-data to automatically produce the XML-Data Schema or the DTD (Document Type Definition) documents. They provide the required reference for the data elements in an XML document and the relationship among the elements, enabling data to be shared across multiple independent parties.

2. Middleware

The definition and categorization of middleware is very broad but can be viewed from two perspectives. From a developer's perspective, middleware is a set of Application Programming Interface (API) calls that can accelerate the development of a distributed system by insulating the developers from the complexities of platform, operating system and software differences associated with a distributed environment. From the perspective of a system architect, middleware is robust connector that integrates a diverse set of solutions that were developed over a period of time, in a distributed environment, into a scalable, reliable and heterogeneous solution. [Britton & Bye] For the purpose of this thesis, a middleware is a set of software that can help bridge two or more applications together and provides interoperability between systems by providing a standard mode of communications between the software from different vendors through some form of conversion or translation mechanism. The complex task of handling differences in operating systems, network, hardware, programming language and data format are encompassed within the set of middleware.

Middleware are useful for the building and integration of distributed applications in a heterogeneous environment. It can manage transaction processing, both in a synchronous and asynchronous settings. It enables information exchange between different systems. Therefore it is able to support the implementation of a technical architecture in a multi-agency setup. Individual agency can continue to maintain their existing IT infrastructure and use one or more middleware solutions to enable interoperability between the various agencies.

Middleware solutions can be classified as follows [Emmerich] :

a. Transactional Middleware

Transactional middleware supports transactions among distributed components through some mechanisms to ensure consistency, like the two-phase commit protocol. There are two approaches to implementing transaction management. The first approach leverages on the transaction management capabilities of the relational database management system. In the second approach, a distributed transaction manager is used so that heterogeneous databases can be updated in a single transaction.

b. Message-Oriented Middleware

Message-Oriented middleware provides an asynchronous messaging model for distributed applications to exchange messages. It can include business logic for routing of messages and reformatting of data. The Message-Oriented middleware is particularly suited for implementing distributed event notification and publish-subscribe mechanism.

c. Procedural Middleware

Procedural middleware primarily deals with synchronous communication between one client and one server through Remote Procedure Call (RPC). Thus, after Procedure A1 from workstation A calls Procedure B2 from workstation B, it waits for the response. Since it uses RPC, Procedural middleware can make use of NDR (Network Data Representation) to define standardized data representation of request and results across heterogeneous environment.

d. Object and Component Middleware

The Object and Component Middleware includes component models like the Common Object Request Broker Architecture (CORBA) from

Object Management Group (OMG), Microsoft's Distributed Component Object Model (DCOM) and Enterprise JavaBeans (EJB) from Sun. This group of middleware can execute processes in real-time and can run anywhere in the network. They integrate the capabilities of the transactional, message-oriented and procedural middleware.

e. Enterprise Application Integration Middleware

Enterprise Application Integration (EAI) middleware allows disparate applications to share information, using adapters that can help convert the native formats of the systems being connected into the canonical protocols and formats being defined at the EAI hub. This will facilitate interoperability between systems of different generations. [Vinoski]

f. Web Services Middleware & XML

Web Services and XML are the latest addition to the class of middleware solution and has been touted as a highly promising technology that can enable seamless interoperability in a heterogeneous computing environment. According to the World Wide Web Consortium (W3C), web service is defined as "*a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically Web Services Description Language WSDL). Other systems interact with the Web service in a manner prescribe by its description using SOAP messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards".* Thus, a web service provides a set of specific functions to its users through well-defined interfaces and encapsulates details of its internal implementation from the user of the service. Though the web service technology is still in its infant stage, it looks extremely promising. The key enabler for web services is the eXtensible Markup Language (XML). XML is a subset of SGML (Standard Generalized Markup Language), an ISO-standard document markup language that has been in used for a number of years. Both the data and the meta-data are embedded in an XML document. All the data in an XML document are represented as character strings. The tags used in an XML document are self-defining and unlimited.

Thus, any form of data can be defined and tailored to the application's need. As long as the sender and the receiver understands a common exchange format through the XML schema or DTD, heterogeneous applications can exchange information and interoperate, independent of operating systems, applications and hardware. The major disadvantage of using XML is the substantial amount of file storage and transmission overheads incurred by maintaining the entire document in text character format together with the meta-data tags.

Choice of Middleware Solution

Since there are many different types of middleware solution all having their respective capabilities and weakness, we will need to align the choice with our requirement in order to find the right middleware solution for the architecture. In the current setup, there are multiple agencies with technologies from various timeframe. There are web-enabled Microsoft and Linux base system. There are also legacy mainframes and minicomputer systems that could have captured 10 to 15 years of information with many supporting applications and business rules closely embedded into the workflow of the agency. One of the key requirements for any new interface into the legacy system is to ensure that it is non-intrusive and will not adversely affect the performance of the existing system.

As the primary objective is to have access to have access to the data sources of multiple agencies and enable data interoperability, Transactional and Procedural Middleware is not required. Most Object and Component middleware are tightly coupled to a specific Operating System platform or programming language and is also more complex to work with. Thus, a Message-Oriented Middleware that can provide the connectors to a diverse set of data sources on many heterogeneous platforms including the legacy mainframe system would be a suitable choice. Some examples of such products are the MQ Series from IBM and SonicMQ from Sonic Software. Keeping in mind the longer term vision of a Service Oriented Architecture where applications from different platforms can interoperate, all information shall be transmitted and stored in XML format. In a Service Oriented Architecture, applications will be running as web services and can be shared across different agencies. For example, a Decision Maker in the ad-hoc task force can execute an application from the Immigration Department to gain more in-depth knowledge of the human traffic at the key entry points into the country, without the need to install another specialized application to get the information.

3. Data Processing Tools

These are specifically developed applications or customized COTS tools that can help to implement the data processing rules that were identified by the Content Managers. Certain information will need to be reformatted to homogenize the different representation that is referring to the same thing or have the same meaning. Reformatting involves the changing of how information of an entity is being presented so that it conforms to the field descriptor in the data dictionary. For example, the different agencies may represent a date field in a variety of formats. There is a need to reformat the date information according to the specification in the data dictionary to facilitate information sharing and downstream automation. Next, data that are not in the standard type may need to be translated accordingly. For example, images that are stored in a proprietary data type may need to be converted to a well known data type like JPG and GIF before it can be shared with other agencies that may be using standard image viewing software and not the specialized software.

The kinds of tools required will largely depend on the format and the type of data. For example, data coming from a relational database would require a SQL-capable data manipulation language for processing and formatting. File content manipulation programs can be developed to process information stored in files, which can include plain text files, word processor documents, PDF documents and spreadsheets.

4. An Example of Data Interoperability Solution

Using the information from the unified data dictionary that maps out the data requirements for the different missions and the location of the data sources to fulfill the data requirement, an application can be developed that leverage on the Message-Oriented Middleware to retrieve the required data from the various data sources. The set of Data Processing Tools will perform the data manipulation operation including, where necessary, reformatting and translating the data. Next, the data will be stored in a common repository as XML documents according to the specified XML Schema or DTD. Subsequently, the XML document will be published onto the Unified Information Bus.

E. ENABLING AD-HOC TEAMS

As discussed earlier, the ad-hoc team can be broken down into four main classes of users. This section will discuss solutions that will be useful for users in a desktop environment, which encompasses the Decision Maker, Operations Coordinator and the Content Manager. Solutions for the Mobile Enforcer will be discussed in the section on Mobile Computing.

1. Situation Collation Manager

The Situation Collation Manager makes use of the defined information profile for a particular user and actively pulls and collates the relevant information from the various data sources through the Unified Information Bus into a comprehensive and relevant situation picture. This can help the users get a quick appreciation of the situation. The information profile of a user specifies the information requirement with respect to the assigned task. One example of how the Situation Collation Manager is useful in the combat against SARS is to ensure that all relevant information of new SARS suspects in a certain area can be automatically collated and routed to the relevant group of users for attention and further actions.

2. Information Dissemination Manager

The Information Dissemination Manager provides an environment for the Operations Coordinator to make use of the information profile associated with a particular user or group of users and configure a set of rules that specifies how information should be shared. The information will then be automatically disseminated according to the stipulated rules. This helps to ensure that relevant information gets routed to the right user in a timely manner.

3. Information Update Tracker

This module will work with the Information Dissemination Manager and is responsible for ensuring that the users operate with the most updated piece of information. Thus, users who had previously received a piece of information gets updated automatically in a timely manner when that piece of information has changed. For example, if an initial report of a suspected SARS outbreak in a certain building is found to be untrue, the Information Update Tracker shall send an immediate update to all the relevant Decision Makers and Operations Coordinator to keep them aware of the changes.

4. Access Control Manager

The Access Control Manager is responsible for ensuring the security of information access by the members of the ad-hoc team. Primarily, it will help to authenticate the users and verify their access rights to the various sources of information. The access rights can be applied to a single user or a group of users. The access rights are assigned through a fine grain access matrix that captures the access of information right down to the fields of the information. It also captures the type of operation the users can perform on the information, by specifying the rights to creating a new piece of information, updating or deleting of information and the right to query the various data sources, including databases and file systems.

5. Search and Query Manager

As there is a need to operate in an unknown situation, the ability to quickly locate the correct piece of information is paramount. The search and query facility is the key to discovering hidden knowledge within the heterogeneous data sources. The Search and Query Manager allows the users to perform both structured and unstructured search through a graphical interface. For structured search, pre-canned queries to specific information sources are provided. This form of query is very useful for sieving information from the databases of the various agencies. For search on unstructured information, one or more key words could be specified and the text search engine will return documents with the exact phrase or documents with phrases that have the same meaning or concept. Thus, with such context sensitive search capability, if we are searching for documents that contain the keyword “pharmacy”, documents containing the phrase “Drug Store”, “Longs” and “Walgreen” will also be returned as part of the result. The search condition can also be configured to only return documents that match exactly the keyword for the search, producing a very specific set of search results. Multimedia information including images, audio and video sources that have been appropriately indexed could also be returned as part of the search results.

The search engine will operate through a direct interface provided by the middleware to the myriad of data sources available. Each user is allowed to query for the information according to the access control matrix captured in the Access Control Manager. The results of the query shall be displayed in a list sorted according to the date and time of the information or the relevancy. Alternatively, the results of the query shall be displayed in a list, sorted by the search criteria of the query that was specified. The users can retrieve the details of the record by clicking on one or more items from the list of results returned from the query.

6. Dynamic Process Manager

The Dynamic Process Manager allows the Operations Coordinator to define the working process for the newly formed ad-hoc organization or team. It can help to capture the roles and responsibilities of all the sub-group in the ad-hoc team. It can also help to describe how the various sub-groups communicate with each other. It defines the information profile for each sub-group, which is the information required by each sub-group to perform its role. It also specifies the information that each sub-group is responsible to produce and share with the rest of the ad-hoc organization. Thus, it captures the set of information to be exchanged amongst the sub-groups. Subsequently, it can automate the dissemination and updating of critical information and orders within the ad-hoc organization with the help of Information Dissemination Manager and the Information Update Tracker. Thus, it provides the complete view of the mode of operation for the ad-hoc organization.

The Dynamic Process Manager can help the members of the ad-hoc team to transit smoothly into their new structure and adjust to the unfamiliar workflow and processes required by their role in the new setup. It works with the Event Alert Manager, the Information Dissemination Manager and the Information Update Tracker to free the team members from consciously ensuring that mundane tasks get the required attention and are handled promptly. Some examples of such tasks includes the monitoring of incoming information for anomalies which could trigger the execution of other actions and the disseminating of new information that one is suppose to share.

7. Event Alert Manager

The Event Alert Manager consists of two key components. The Event Manager helps in the capturing of significant events that requires monitoring. The Alert Manager will actively monitor the incoming information and alert the end user when the defined threshold is breached.

Both the modules can be integrated into a responsive and powerful solution to help in the combat of SARS. For example, there may be a need to implement the rule that all newly discharged patients or SARS suspect from Tan Tock Seng Hospital can only return to the same hospital for medical treatment within 21 days of their discharge. The rule can be defined in the Event Manager, by capturing the key attributes that defines this event including the patient's record together with the validity period for this event, which in this example is 21 days. As the set of modules is operated in a distributed environment supported by a robust middleware for the exchange of critical information, the Alert Manager of other hospitals will use the event defined in the Event Manager at Tan Tock Seng Hospital to automatically monitor the personal information of incoming patients and alert the respective hospital registrar when the rule is breached. Thus, these modules can work together to ensure that patients will not be able to violate the rule and potentially bring the SARS infection into another hospital. These solutions can be extended to alert all medical practitioners in private clinics. Similarly, inter-agency coordination can be further enhanced if the events defined at Tan Tock Seng hospital can be monitored by the Alert Manager operated at the immigration department to ensure that the SARS patient cannot leave the country while there is still a risk of spreading the infection.

8. Collaboration Tools

The collaboration tools allow the different users in the ad-hoc organization to work together in real-time to do planning, resolve any exigencies and conflicts in resource allocation and complete the required group tasking in the most optimal manner. Such a collaborative environment would also be the backbone that facilitates the group decision making process as it provides the means to discuss and arrive at a decision. A computerized whiteboard can be used as a medium where the various stakeholders can come together to share information and rationalize their thoughts in real time, without the need for a face to face meeting. Such collaboration environment also helps disparate groups of people to be linked together and maintain a common situational awareness. It also helps geographically dispersed personnel exchange knowledge, co-ordinate actions and effect decisions efficiently.

9. Analysis & Simulation Tools

This is an interface to a set of tools that supports analysis and decision making for the combat of asymmetric threats like the SARS outbreak.

The Link Analysis Tool allows users to retrieve information on key entities and links and graphically model them so that decision makers can get a graphical view of how the various factors interact and get a better understanding of the complex relationship amongst the entities. This helps to unveil evidence that were not apparent when looking at them in isolation, as a single piece of information. In the combat of SARS, the Link Analysis Tool can help to correlate the critical elements in the disease network. It can also be used to trace the spread of the virus, providing the critical information required for contact tracing of SARS suspect.

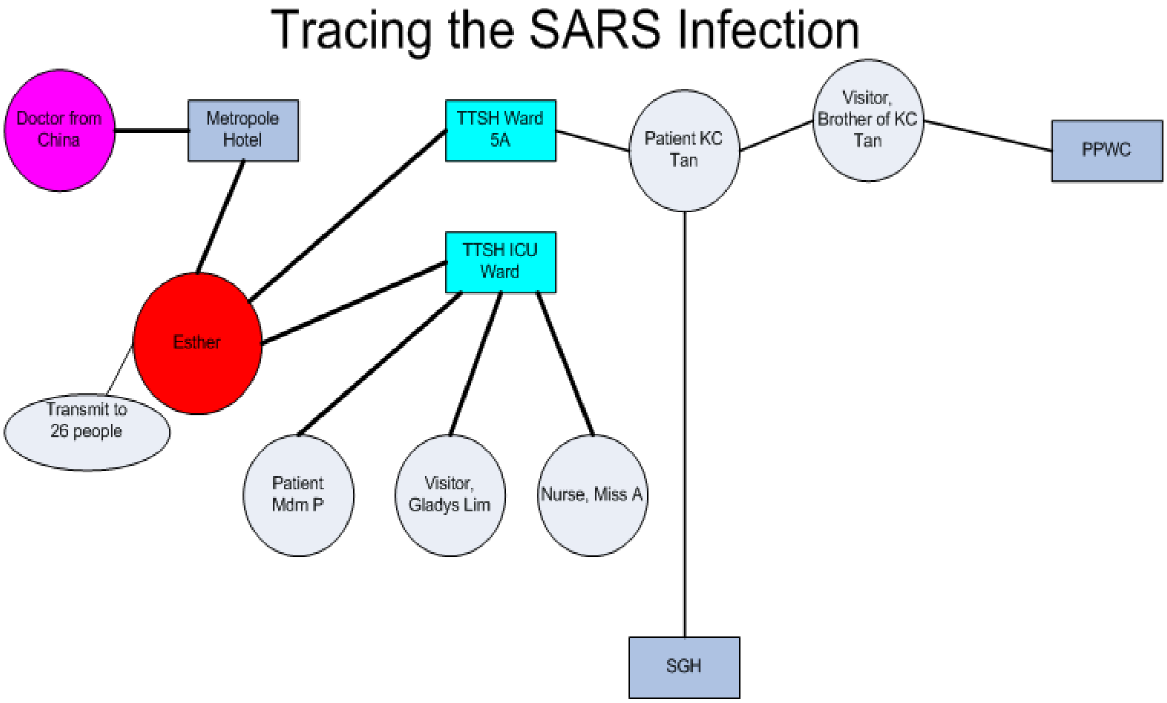

Figure 11. Example of using Link Analysis Tool to trace the SARS Infection

As there is a need to deal with the unknown which is a key characteristic of asymmetric threats, having an interface to access a Modeling and Simulation environment can be useful for analyzing the effects of future plans and understanding the behavior of the disease. The simulation test-bed can provide a controlled environment for users to rapidly obtain the required results by executing the plans over compressed time. It allows one to perform sensitivity analysis and is a good training tool. Thus, decision makers can be better equipped to tackle issues concerning resource allocation and optimization, capacity planning, detection of bottlenecks, validation and comparison of execution plans. The Modeling and Simulation environment can help the users to learn, train and evolve their strategies to better prepare them in dealing with the rapidly changing situations. In the combat of SARS, having a simulation environment that can accurately model the spread of the virus will greatly help in the development and evaluation of the various disease containment strategies.

F. SUPPORT FOR MOBILE COMPUTING

To be effective in the combat of asymmetric threats in an urban environment, the ability to support the needs of the mobile users is important. There will be a lot of mobile teams moving in the city performing a variety of task that can include rescue work, law enforcement, information gathering or directly dealing with the threat. Having the ability to communicate and collaborate while on the move will enable them to perform their duties well. It is crucial for the mobile users to be able to receive mission critical information and send situation updates in real time, working within the constraints of the mobile device, communication infrastructure and bandwidth.

1. Mobile Gateway Module

The Mobile Gateway Module is a series of software responsible for ensuring that all the mobile users can securely and efficiently gain access to the information services that is required for their task. It also processes the incoming messages from the mobile users.

The module will authenticate users and check their access rights to the information services. It has the ability to serve information to a series of PDAs and WAP-enabled devices by ensuring that the XML encoded content gets translated into the markup language that the requesting mobile device can process. Thus, the information can be served in HTML, WML, CHTML and XHTML. Through this module, users can access the information at any place and at any time, by the executing the required JSP or ASP script.

2. Priority Information Alert Service.

The Priority Information Alert Service allows the mobile users to receive mission related information while on the move. The type of information that is served to the user includes tasking orders, situation reports and a host of local information for weather, traffic and critical news.

3. Mapping Information Services

The Mapping Information service provides street maps and terrain features for the area that the mobile users need to operate in. This allows the mobile users to access maps and terrain information using their mobile device like the PocketPC and WAP-based handhelds, while on the move. 2nd level information containing further description of the area is also available.

Equipped with this capability, the mobile users can now find out the exact location of a building, the suggested path for him to expeditiously get there, and the locations of the nearest amenities and essential services.

4. Mobile Reporting Module

This module allows the mobile user to send structured reports of ground situation back to the Operations Coordinator in the Command Centre through their mobile device. It also facilitates collaboration by providing the capability to send unstructured instant messages to other team members, for real time exchange of critical information.

5. Infrastructure for Mobile Communication

In an emergency situation, the communication infrastructure would expect a surge in workload. In order to be more equipped in dealing with a variety of asymmetric threats, it may be necessary to have a dedicated communication infrastructure. Thus, it is worth exploring the possibility of setting up a separate Metropolitan Area Network (MAN) within an urban city, to serve the needs of law enforcement officers, ad-hoc task force and first responders including firemen and rescue workers. Such a network can help ensure persistency in connectivity, with seamless and automatic switching between disparate networks. Therefore, even at the peak of a crisis, the mobile teams can continue to receive tasking orders and situation reports from the Command Centre. They can continue sending timely ground situation reports and communicate with their peers.

An example of a wireless Metropolitan Area Network is shown in Figure 12.

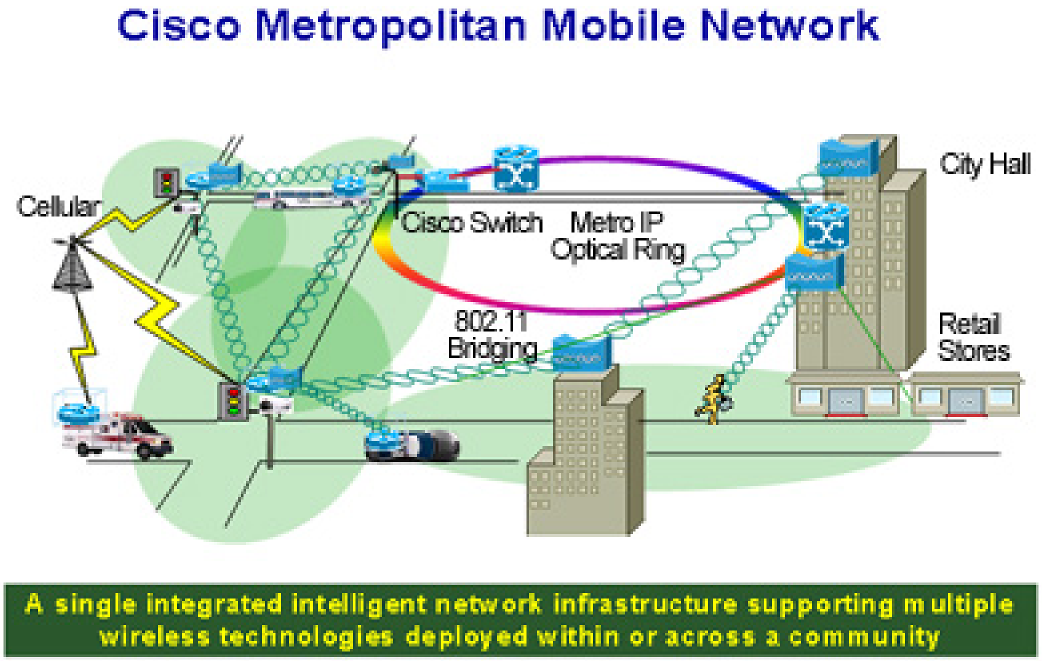
Cisco Metropolitan Mobile Network
Cellular
Cisco Switch
Metro IP
Optical Ring
City Hall
802.11
Bridging
Retail
Stores
A single integrated intelligent network infrastructure supporting multiple wireless technologies deployed within or across a community

Figure 12. Example of Wireless Metropolitan Area Network. [Cisco]

A series of WLAN routers is mounted in prominent places within the city, including lamp post along the road, top of buildings and bridges. This series of routers and access points will form the Metropolitan Area Network. A mobile user whose device is within the range of the wireless access point will have the network automatically initiate a session to exchange information. If the user leaves the network in the middle of the session, into an area with restricted or no communications bandwidth, the point of interruption is recorded so that the remaining data can be delivered in the next instance when the mobile user is within the network range where there is sufficient bandwidth to complete the operation.

G. CONCLUSION

In this chapter, an architecture was proposed to ensure that a network of distributed organization components comprising of fixed and mobile elements can interoperate by exchanging information and coordinate activities in a flexible and scaleable manner. The architecture amalgamates a set of software and information services and focus on three critical areas, namely: Data Interoperability, Support for Ad-Hoc Organization and Mobile Computing.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION AND FUTURE WORK

A. CONCLUSION

This thesis takes a retrospective view of the SARS incident in Singapore and discusses how Network Centric Operation concepts can be applied to deal with such a disease outbreak and similar kinds of biological asymmetric threats. Hitherto, discussions on the applications of Network Centric Warfare (NCW) have been skewed towards the needs of the military and build on the assumptions of the military. Employing the NCW framework to deal with an unconventional crisis brought on by an asymmetric threat that requires close coordination between multiple agencies including many non-military organizations to deal with it revealed several unique insights.

In general, this category of asymmetric threats can be characterized by events that are out of the ordinary with no precedence, having many complex and evolving problems emerging in a time critical and rapidly deteriorating environment. There can be many new and unknown factors involved, and the relationships among them are unclear.

The key NCW lessons learnt from the Singapore's SARS incident include:

- The importance of information sharing.
- The need to setup and work with an ad-hoc and flexible organizational structure.
- The need for interoperability of inter-agency processes
- The need to support mobility and agility
- The need for pragmatic employment of technology

Three main technological areas have been identified to be crucial in ensuring that seamless interoperability amongst the various agencies can be achieved. These are data interoperability, support for ad-hoc organization and mobile computing. Subsequently, a technical architecture that amalgamates a set of software and information services that encompasses the three identified areas was proposed. This architecture enables seamless sharing of information from heterogeneous sources and organizations. It also enhances the interoperability of the ad-hoc multi-agency teams. The architecture can help to facilitate decision making and ensure that timely response can be executed in the combat of the asymmetric threat. The architecture is designed serve the needs of the four classes of users that was identified in the thesis. They include the strategic decision makers, the operations coordinator, the mobile enforcers and the content managers. It is recommended that the software solutions within the three different parts of the architecture be developed in parallel and verification exercises be setup to demonstrate how the various sub-modules can work together to deal with asymmetric threats.

B. ENHANCEMENTS TO THE TECHNICAL ARCHITECTURE

There are several other potentially high payoff areas that have been identified and should be further explored. These include:

1. Service Oriented Architecture

One of the solutions to support data interoperability for the current proposed architecture is to setup a common data repository that standardizes the information required and available for the various missions in the combat of unconventional asymmetric threats. XML is the standard format used to support all storage and transmission of the required information. The current setup can be further enhanced into service oriented architecture by converting the set of proposed solutions into web services. This can help to explore and demonstrate the viability of implementing a large scale service oriented architecture that supports disparate group of users from multiple agencies. The effort can also help to explore the possibility of handling real-time and non-real-time requirements together using a service oriented architecture. The most notable contribution from this effort will be the ability to demonstrate seamless access to multiple data sources and applications from a ubiquitous web based interface.

2. Security Services

This enhancement involves a review of the security requirements and a study of the security policies, controls, tools and mechanisms required to support a multi-agency ad-hoc task force. There are different technologies, system and platforms involved. The objective is to ensure that all users of the services and software tools on the architecture can be appropriately authenticated and accounted. It also ensures that all information can be securely stored and communicated by designing security solutions to protect the information from unauthorized disclosure, modification, interference and destruction. The required security services for both the desktop and the mobile users can be subsequently developed and incorporated into the architecture.

3. Information Exploitation Services

Implementing the current architecture helps to ensure that data interoperability can be achieved and seamless cross agency access to data is enabled. This provides the ability to share information and attain a common level of situation awareness. The next important milestone would be to explore techniques and tools that can enhance the exploitation of the vast amounts of information available. This can help the users search and navigate through large volumes of data sources and perform text mining to discover patterns, unveil hidden relationships, cluster related information and create linkages between disparate pieces of information and transform them into useful knowledge that can be appropriately tagged and stored. This area of work also includes finding the most optimal strategy to extract, represent, store, exploit and present the different types of information available including Abstract Information, Executive Information and Specific Information. There may be other effective solutions for capturing and representing the tacit knowledge residing in the minds of the decision makers, which will be extremely useful if it can be extracted, represented and stored into knowledge bases for sharing, query and further analysis.

4. Information Presentation Services

With seamless access to the vast amount of information from the large network of data sources, information presentation and navigation becomes a key capability in the management of content overload and ensure that the information are being presented within the context of the user. This area of work shall explore effective techniques for information presentation and navigation which could include the use of animation, audio and video means, suitable highlights and alarms, multiple integrated views of the information and content summary in an attempt to find the most optimal way of presenting information according to the task, the need and the capability of the computing device.

Another important area of work is to explore new ways of presenting information on small handheld device like personal digital assistance (PDAs) and possibly 3G cellular phones, when used in a rapidly changing and time critical environment that characterize the combat against an asymmetric threat. Handheld devices also help team members maintain situation awareness and facilitate decision making while on the move These devices have other unique characteristics in terms of computation power, networking capabilities, display size and battery life, that further constraint the type of solutions that can be developed. Thus, there is a need to investigate the most optimal way to present alerts and updates and to enable collaboration among team members.

5. Mobile Computing Services

This study shall involve further explorations of the mobile computing services that will be useful in enabling decision making on the move and ensuring timely and precise response for the mobile enforcers. Extending beyond the scope of the SARS incident in Singapore, to be truly mobile and able to support the deployment of an ad-hoc task force to any place at any time, there is a need to explore other options of providing the infrastructure required for mobile communication and implement an equivalent of a Metropolitan Network using mobile infrastructure. In terms of information management and decision support, there is a need to explore the various techniques for information presentation, delivery and synchronization for mobile users by taking into consideration the capability of the mobile devices that the end user carry, and the various physical and ergonomics factor associated with the mobile device. There is also a need to explore strategies to provide reliable access to information while on the move.

C. EXPLORATION ON COGNITIVE SERVICES

Cognitive services can help Decision Makers analyze data, assess various hypotheses, consider alternatives and make decisions. The objective of the study is to explore the following cognitive tools and assess its usefulness in the combat of asymmetric threats:

1. Analysis Tools

This set of tools allows the user to integrate and correlate information from different sources and perform time, space and activity analysis. Performing time analysis allows the user to understand the critical path and timeline of the various events. Performing space analysis allows users to explore and better understand location-centric events. Performing activity analysis allows the users to gain insights of critical processes associated with the asymmetric threat in the given time and space. All the tools can work together and help the users gain a better understanding of the complex relationship among activities and events that would otherwise appear unrelated.

2. Hypothesis Tools

The hypothesis tool allows the users to map out all the possible causes of action or hypotheses, for the event associated with the existing asymmetric threat that is being dealt with. Subsequently, incoming data and evidence collected can help to substantiate or eliminate some of the hypotheses. It also allows users to compare and evaluate the alternative causes of actions.

D. SIGNIFICANCE OF THE SOCIAL NETWORKS

The success of Network Centric Operations is not just dependent on technology and process. The most significant contribution and impact will come from the people involved. Thus, there is a need to explore and gain a better understanding of how social networks and organization dynamics can influence the success of Network Centric Operations. By investigating on the desired set of behavioral traits and organization structure, we will have the right setup and be more equipped to leverage on social networks to reinforce the capability of the Network Centric Operations.

Beside formal structures, research could include how informal networks within groups of people determine the performance of the groups. Research in this area could include how such informal networks are formed; why and how a person associates with such informal networks; how individuals behaves within such informal networks and how such behaviors affect the outcome of the network.

Studies into the contributions of formal structures and informal networks toward the objective of the group could be carried out. Such studies will help determine the positive and negative effects of these networks; how one can design formal structures and facilitate the formation of informal networks that will compliment rather than negate each other.

With this analysis, we will have a better understanding of how collaborations happen within networks. This will help the formulation of tools and procedures that will facilitate and supplement these collaborative processes.

THIS PAGE INTENTIONALLY LEFT BLANK

BIBLIOGRAPHY

[1] Mui Hoong, Chua. A Defining Moment: How Singapore Beat SARS. Institute of Policy Studies, July 2004.

[2] John J. Garstka, David S. Alberts. Network Centric Operations Conceptual Framework Version 2.0 CRIP June 2004.

[3] John J. Garskta, David S. Alberts, Frederick P. Stein. Network Centric Warfare : Developing and Leveraging Information Superiority, National Defense University Press 1999.

[4] www.sars.gov.sg Singapore web site for SARS, December 2004

[5] PA Cosulting Group. A Network Centric Operations Case Study: US/UK Coalition Combat Operations during Operation Iraqi Freedom, June 23 2004

[6] Highlands Forum Interview with Dr Sudderuddin, March 2004

[7] Jody Lanard M.D. "Singapore's SARS Outbreak Communications". WHO Expert Consultation on Outbreak Communications, Singapore 21 September 2004.

[8] Chris Britton, Peter Bye. IT Architecture and middleware: Strategies for building large, integrated systems, Addison Wesley 2004.

[9] Waltz Edward. Knowledge management in the intelligence enterprise, Artech House INC 2003.

[10] Steve Vinoski. An Overview of Middleware. Ada-Europe 2004.

[11]www.cisco.com/en/US/netsol/ns473/networking_solutions_package.html. ,November 2004

[12] Yong Ying-I, Singapore One The Vision of An Intelligent Island, ,http://www.ida.gov.sg/idaweb/media/infopage.jsp?infopagecategory=general.speeches:media&versionid=4&infopageid=I690 , November 2004

[13] K.J. Radford. Complex Decision Problems: an Integrated Strategy for Resolution. Virginia: Prentice-Hall Company, 1997.

[14] C.F Kurtz, D.J. Snowden. The new dynamics of strategy: Sense-making in a Complex and Complicated World. IBM Systems Journal Vol 42, No 3, 2003.

[15] M. Mitchell Waldrop. Can Sense-making Keep us Safe? Technology Review. March 2003.

[16] Albert-Lazzlo Barabasi. Linked: How everything is connected to everything else and what it means. Perseus Publishing, 2002.

[17] Gerd Gigerenzer & Peter M. Told. Simple Heuristics That Make Us Smart. Oxford: Oxford University Press, 1999.

[18] Rob L. Cross & Andrew Parker. The Hidden Power of Social Networks: Understanding How Work Really Gets Done in Organizations. Harvard Business School Press, 2004.

[19] Russel M. Linden. Working Across Boundaries: Making Collaboration Work in Government and Nonprofit Organization. Jossey-Bass, 2002.

[20] Klaus Mainzer. Thinking in Complexity: The Computational Dynamics of Matter, Mind and Mankind (4th edn). Springer-Verlag Berlin, 2004.

[21] Cebrowske. Speech to Network Centric Warfare 2003 Conference, 22 Jan 2003.

[22] Hon Robert Hill. Network Centric Warfare: Address to the ADF Network Centric Warfare Conference, 20 May 2003.

[23] John Khil. Future Trends in Network Centric Warfare. Swedish Armed Forces, 2003.

[24] Wolfgang Emmerich. Software Engineering and Middleware: A Roadmap. ICSE2000 ACM Press, May 2000.

[25] Robert Popp, Thomas Armour, Ted Senator, Kristen Numrych. Countering Terrorism Through Information Technology. Communications of The ACM, Vol 47, No 3.

[26] Straits Times Commentary by M Nirmala. "We are open transparent… We cannot hide what goes on in Singapore", May 18 2003.

[27]. Straits Times Commentary by Susan Long. "Singapore at War", May 11 2003.

[28] Straits Times Commentary by Andy Ho. "What if bio-terrorists strike in S'pore", May 16 2003

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. BG Jimmy Khoo
   Future System Architect
   Future System Directorate, MINDEF.
   Singapore

4. Mr John J. Garstka
   Assistance Director for Concepts and Operations
   Office of Force Transformation, Office of Secretary of Defense

5. Prof Yeo Tat Soon
   Vice Dean, Engineering Faculty/
   Director, Temasek Defence Systems Institute
   National University Singapore, Singapore

6. Prof Susan Higgins
   Deputy Director, Cebrowski Institute for Information Innovation and Superiority
   Naval Postgraduate School
   Monterey, California